

RADIO ACCESS NETWORK, MULTIHOPPING RADIO NETWORK, AUTHENTICATION SERVER, BASE STATION AND RADIO TERMINAL

Publication number: JP2003249944 (A)

Also published as:

Publication date: 2003-09-05

JP3880419 (B2)

Inventor(s): NIHEI KATSUTOSHI; YOSHINO SHUICHI; NAKAYAMA MASAYOSHI; SUDA HIROTO

Applicant(s): NIPPON TELEGRAPH & TELEPHONE

Classification:

- international: H04L9/32; H04L12/56; H04Q7/38; H04L9/32; H04L12/56; H04Q7/38; (IPC1-7): H04L12/56; H04L9/32; H04Q7/38

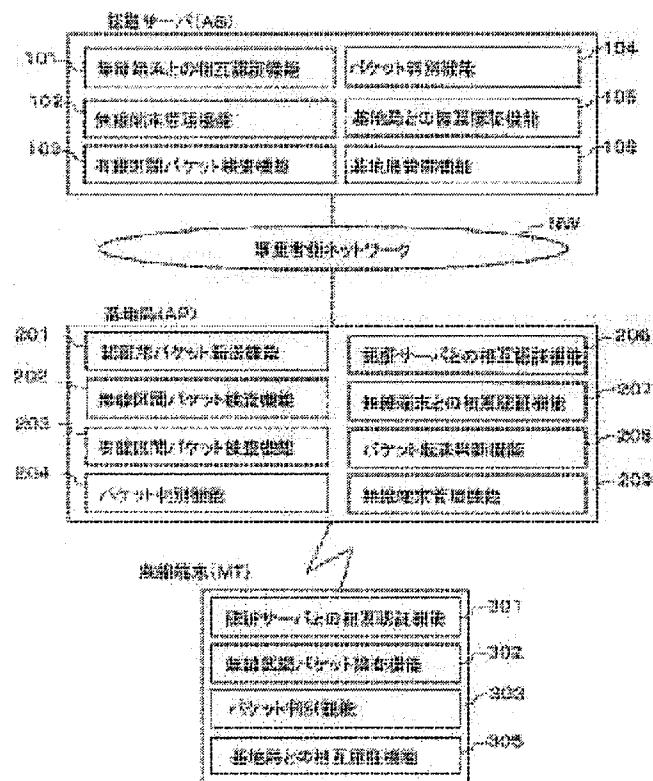
- European:

Application number: JP20020045240 20020221

Priority number(s): JP20020045240 20020221

Abstract of JP 2003249944 (A)

PROBLEM TO BE SOLVED: To provide a technique having excellent resistance to a DoS (Denial of Service) attack in a radio access network and a multihopping radio network.



Data supplied from the esp@cenet database — Worldwide

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-249944

(P2003-249944A)

(43)公開日 平成15年9月5日 (2003.9.5)

(51)Int.Cl.⁷
H 0 4 L 12/56
9/32
H 0 4 Q 7/38

識別記号

F I
H 0 4 L 12/56
9/00
H 0 4 B 7/26

テ-マコード(参考)
A 5 J 1 0 4
6 7 5 D 5 K 0 3 0
1 0 9 R 5 K 0 6 7

審査請求 未請求 請求項の数18 O.L (全 42 頁)

(21)出願番号 特願2002-45240(P2002-45240)
(22)出願日 平成14年2月21日 (2002.2.21)

(71)出願人 000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号
(72)発明者 仁平 勝利
東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
(72)発明者 吉野 修一
東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
(74)代理人 100083806
弁理士 三好 秀和 (外1名)

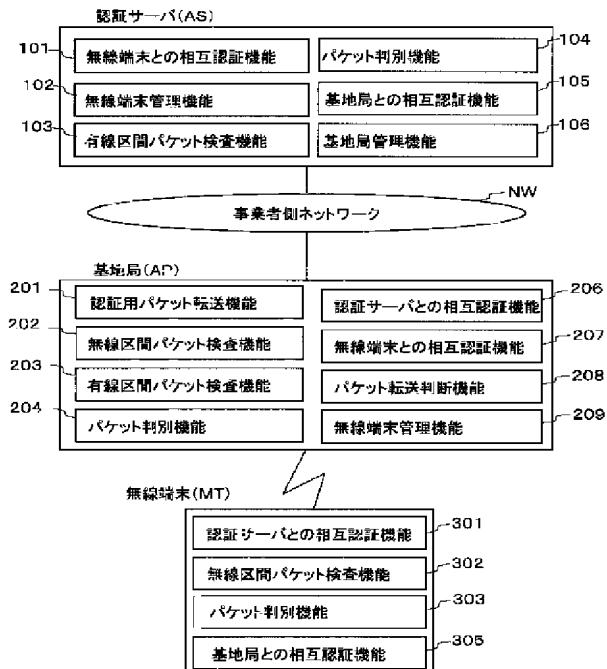
最終頁に統く

(54)【発明の名称】 無線アクセスマルチホップネットワーク、認証サーバ、基地局及び無線端末

(57)【要約】

【課題】 無線アクセスマルチホップネットワークにおいて、DOS攻撃に対する耐性に優れた技術を提供する。

【解決手段】 認証サーバ (AS) と新規な基地局 (AP) が相互認証を行うことで、事業者が一般ユーザの設置したAPの安全性を保障する。また新規無線端末 (MT) がアクセスしたとき、最初にMT-AP間で相互認証することで互いが正当な装置であるか否かを確認し、APはこの相互認証が成功するまでは新規MTが送信したパケットを事業者側ネットワークに転送しないようにすることにより、認証を装ったDOS攻撃を防止する。さらに、MT-AP間の相互認証成功後にMT-AS間の相互認証及びこの認証用パケットのパケット検査 (送信元確認) を行うことでASはどのAPにどのMTがアクセスしたかを正確に把握する。



【特許請求の範囲】

- 【請求項1】 無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセスネットワークにおいて、
- A. 前記基地局は、前記事業者側ネットワークに新規に接続するときに基地局一認証サーバ間認証用パケットを送信して前記認証サーバと相互認証を行う処理機能、
 - B. 前記無線端末は、当該無線アクセスネットワークに新規にアクセスするときに近隣にある基地局と相互認証を行い、認証成功後に無線端末一認証サーバ間認証用パケットを送信し、前記基地局は、前記無線端末との相互認証が成功したときに当該無線端末から送信されてきた前記無線端末一認証サーバ間認証用パケットの転送を許可し、前記認証サーバは、前記無線端末一認証サーバ間認証用パケットにより前記基地局を介して前記無線端末と相互認証を行う処理機能、
 - C. 前記無線端末、基地局、認証サーバそれぞれは、前記無線端末一認証サーバ間認証用パケットを送信し又は転送するときに送信元を示すパケット検査データを当該認証用パケットに添付する処理機能、
 - D. 前記無線端末、基地局、認証サーバそれぞれは、前記無線端末一認証サーバ間認証用パケットを受信したときに、それに添付されているパケット検査データを検査し、当該検査が失敗した場合はそれが添付されている認証用パケットを破棄する処理機能、
 - E. 前記認証サーバは認証した新規の基地局、新規の無線端末それぞれの情報を自装置に登録する処理機能を備えたことを特徴とする無線アクセスネットワーク。
- 【請求項2】 中継能力を持つ無線端末と、この無線端末と無線通信する基地局と、この基地局と事業者側ネットワークを通じて接続される認証サーバとから構成される無線マルチホップネットワークにおいて、
- A. 前記基地局は、新規に事業者側ネットワークに接続するときに前記認証サーバと基地局一認証サーバ間認証用パケットを用いて相互認証を行う処理機能、
 - B. 前記無線端末は、新規に当該無線マルチホップネットワークにアクセスするときに近隣の認証済みの無線端末又は基地局と無線端末間認証用パケットによって相互認証を行う処理機能、
 - C. 前記無線端末間の相互認証が成功した無線端末又は基地局が複数あれば、その中から1つの無線端末又は基地局を選択し、前記選択された無線端末又は基地局は、前記新規無線端末から送信された無線端末一認証サーバ間認証用パケットの転送を許可する処理機能、
 - D. 前記新規無線端末は、前記無線端末間の相互認証の成功後に、無線端末一認証サーバ間認証用パケットを用い、選択した無線端末又は基地局を経由して前記認証サーバと相互認証を行う処理機能、
 - E. 前記新規無線端末、選択された無線端末、基地局、

認証サーバそれぞれは、前記無線端末一認証サーバ間認証用パケットを送信し又は転送するときに送信元を示すパケット検査データを当該認証用パケットに添付する処理機能、

F. 前記新規無線端末、選択された無線端末、基地局、認証サーバそれぞれは、前記無線端末一認証サーバ間認証用パケットを受信したときに、それに添付されているパケット検査データを検査し、当該検査が失敗した場合はそれが添付されている認証用パケットを破棄する処理機能、

G. 前記認証サーバは相互認証に成功した新規の基地局、新規の無線端末それぞれの情報を自装置に登録する処理機能を備えたことを特徴とする無線マルチホップネットワーク。

【請求項3】 無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセスネットワークに用いられる無線端末であって、前記無線アクセスネットワークに新規にアクセスするときに、無線端末一基地局間認証用パケットを送信して近隣の基地局と相互認証を行い、認証成功後に無線端末一認証サーバ間認証用パケットを送信し、認証サーバとの間で相互認証を行う機能を備えたことを特徴とする無線端末。

【請求項4】 送信する無線端末一認証サーバ間認証用パケットに送信元を示すパケット検査データを算出して添付する機能を備えた請求項3に記載の無線端末。

【請求項5】 前記無線端末一基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、無線端末一基地局間認証において正当な1つの基地局を選択し、当該基地局を通じて前記無線端末一認証サーバ間認証用パケットを前記認証サーバに送信する機能を備えたことを特徴とする請求項3又は4に記載の無線端末。

【請求項6】 前記無線端末一基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、応答の早い基地局から優先的に選択して無線端末一基地局間認証を実行する機能を備えたことを特徴とする請求項5に記載の無線端末。

【請求項7】 前記無線端末一基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、応答信号の受信レベルの強い基地局から優先的に選択して無線端末一基地局間認証を実行する機能を備えたことを特徴とする請求項5に記載の無線端末。

【請求項8】 前記無線端末一基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、各基地局との無線端末一基地局間の認証手続きにおいて取得した情報に基づき、正当な基地局を選択する機能を備えたことを特徴とする請求項5に記載の無線端末。

【請求項9】 無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワーク

で接続された認証サーバとから構成される無線アクセスネットワーク又は無線マルチアクセスネットワークに用いられる認証サーバであって、

新規にアクセスしてきた基地局と相互認証を実行し、認証が成功した基地局の情報を自装置に登録する機能と、無線端末ー認証サーバ間認証用パケットにパケット検査データを添付して基地局に送信し、基地局から送られてきた無線端末ー認証サーバ間認証用パケットに添付されているパケット検査データを検査し、検査が失敗した場合はそのパケットを破棄し、この検査が成功すれば無線端末との相互認証を実施し、相互認証に成功した無線端末の情報を自装置に登録する機能を備えたことを特徴とする認証サーバ。

【請求項10】 相互認証に成功した無線端末が別の基地局の通信エリアへ移動したとき、当該無線端末との新たな相互認証を実施し、認証が成功した後に当該無線端末の属していた旧基地局へその無線端末が移動したことを通知する機能を備えたことを特徴とする請求項9に記載の認証サーバ。

【請求項11】 無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセスネットワーク又は無線マルチホップネットワークにおいて用いられる基地局であって、

新規に前記無線アクセスネットワーク又は無線マルチホップネットワークに接続したときに、基地局ー認証サーバ間認証用パケットを前記認証サーバに送信して相互認証を実行する機能を備えたことを特徴とする基地局。

【請求項12】 新規の無線端末からの無線端末ー基地局間認証要求に対して相互認証を行い、当該相互認証が成功したときに当該無線端末から送信されてきた無線端末ー認証サーバ間認証用パケットに対して、それに添付されているパケット検査データを検査し、検査が失敗した場合はそのパケットを破棄し、当該検査が成功すれば、当該無線端末ー認証サーバ間認証用パケットを、自装置で算出したパケット検査データを添付して認証サーバに転送し、認証サーバから送信されてきた認証用パケットに示されている認証結果を参照して新規無線端末が送信したすべてのパケットの事業者側ネットワークへの転送を許可するか否かを判定する機能を備えたことを特徴とする請求項11に記載の基地局。

【請求項13】 相互認証に成功した無線端末それぞれの情報を自装置に登録する機能と、認証サーバから移動通知を受けて、該当する無線端末の登録情報を削除する機能とを備えたことを特徴とする請求項11又は12に記載の基地局。

【請求項14】 中継能力を持つ無線端末と、この無線端末と無線通信する基地局と、この基地局と事業者側ネットワークを通じて接続される認証サーバとから構成される無線マルチホップネットワークにおいて用いられる

無線端末であって、

自装置が新規に無線マルチホップネットワークにアクセスするときには近隣の認証済みの他の無線端末又は基地局と相互認証を行い、複数の無線端末又は基地局と相互認証が成功した場合、正当な1つの無線端末又は基地局をプロキシ端末として選択し、当該プロキシ端末を介して認証サーバとの相互認証を実行する機能と、自装置が他の新規無線端末によって選択されたプロキシ端末である場合には、他の新規無線端末から送信された新規無線端末ー認証サーバ間認証用パケットをルート上の他の無線端末又は基地局に対して転送する機能とを備えたことを特徴とする無線端末。

【請求項15】 自装置が新規に無線マルチホップネットワークにアクセスするときには、無線端末間認証用パケットを近隣の他の無線端末又は基地局に送信する機能と、

自装置が新規無線端末である場合に、無線端末ー認証サーバ間認証用パケットに送信元を示すパケット検査データを添付して送信する機能と、

自装置が他の新規無線端末によって選択されたプロキシ端末である場合には、他の新規無線端末又は基地局から送信された無線端末ー認証サーバ間認証用パケットに対してパケット検査データを検査し、検査が失敗すればその認証用パケットを破棄し、当該検査が成功すれば当該認証用パケットに自装置で算出した送信元を示すパケット検査データを添付してルート上の他の無線端末又は基地局に対して転送する機能とを備えたことを特徴とする請求項14に記載の無線端末。

【請求項16】 基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局から応答を受けたとき、応答の早い基地局又は他の無線端末から優先的にプロキシ端末として選択する機能を備えたことを特徴とする請求項14又は15に記載の無線端末。

【請求項17】 基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局から応答を受けたとき、受信レベルの強い基地局又は他の無線端末から優先的にプロキシ端末として選択する機能を備えたことを特徴とする請求項14又は15に記載の無線端末。

【請求項18】 基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局から応答を受けたとき、相互認証で取得した他の無線端末又は基地局の情報に基づいてプロキシ端末を選択する機能を備えたことを特徴とする請求項14又は15に記載の無線端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は基地局を介して有線ネットワークに接続される無線アクセスネットワーク又は無線マルチホップネットワークにおいて、無線端末及

び基地局の認証を行う認証方法に関するものである。

【0002】

【従来の技術】図50に認証サーバ(A S : Authentication Server)を用いた無線アクセシティネットワークの一般的な機能構成を示してある。この無線アクセシティネットワークは、無線端末MT(Mobile Terminal)、この無線端末MTと無線通信する基地局AP(Access Point)、この基地局APと事業者側有線ネットワークNWを通じて接続される認証サーバASから構成される。

【0003】認証サーバASはソフトウェアとして、無線端末MTとの相互認証を実行する無線端末との認証機能101、認証した無線端末MTをデータベースに登録して管理する無線端末管理機能102、ネットワークNWのパケットを検査する有線区間パケット検査機能103、パケット判別を行うパケット判別機能104を備えている。

【0004】基地局APはソフトウェアとして、認証サーバASと無線端末MT間の認証用パケットの転送を行う認証用パケット転送機能201、無線ネットワークのパケットを検査する無線区間パケット検査機能202、有線ネットワークNWのパケットを検査する有線区間パケット検査機能203、パケット判別を行うパケット判別機能204を備えている。

【0005】無線端末MTはソフトウェアとして、認証サーバASとの相互認証を実行する認証サーバとの相互認証機能301、無線ネットワークのパケットを検査する無線区間パケット検査機能302、パケット判別を行うパケット判別機能303を備えている。

【0006】この提案されている無線アクセシティネットワークでは、ある無線端末MTがそのネットワークにアクセスするとき、MTは基地局APを介してASと相互認証を行う。基地局APは、無線端末MTから受信した認証用パケットを終端して認証サーバASへ転送し、また認証サーバASから受信した認証用パケットを無線端末MTへ転送する。認証サーバASによる無線端末MTの認証が成功したら、基地局APに対してそのMTから無線送信されてきたデータパケットを事業者側ネットワークNWへの転送を許可し、無線端末MTから事業者用ネットワークNW上の他の接続端末へのアクセスを可能にする。

【0007】

【発明が解決しようとする課題】このような無線アクセシティネットワークでは、基地局APが会社内等の限定されたアクセス環境ではなく、屋外等の誰でも容易にアクセスできる環境に設置されることが特徴であるが、そのような場合は、図51に示したように、悪意あるユーザが無線端末MTの認証を装って大量にパケットを送信することによって認証サーバASをダウンさせることができるものである。このようなDenial of Service

(D o S)攻撃をされた場合、その無線アクセシティネットワークへ新規ユーザが無線端末MTによってアクセスすることが不可能になる。

【0008】一方、事業者ではなく、一般ユーザが基地局APを設置した場合、認証サーバASでは新規の基地局APの認証を行わないため、事業者がそうしたAPのセキュリティ機能を保障することが不可能となる。そのため、一般ユーザが設置したAPには、他ユーザが安心してアクセスすることができない。その上、基地局APの認証がない場合、基地局APから送信されたトラヒック情報や課金情報等の正当性も確認できないので問題となる。

【0009】また、一般ユーザが基地局APを設置した場合、図52に示したように、APの設置密度が高くなって1つの無線端末MTが複数の基地局AP # iとAP # jとに同時にアクセス可能になることも考えられる。こうした環境では、無線端末MTが同時に複数のAPを介して認証サーバと認証を行うことになり、同じ認証処理が同時に発生してしまう問題がある。

【0010】この同時認証処理が発生する問題は、各々の無線端末MTが中継機能を持つ無線マルチホップネットワークにおいて顕著となる。図53に無線マルチホップネットワークの機能構成例を示してある。この無線マルチホップネットワークでは、基地局APがパケット中継機能205を追加的に備え、また無線端末MTもパケット中継機能304を追加的に備えている。そして、図53に示した無線マルチホップネットワークでは、例えば、無線端末MT7は、他の無線端末MT6, MT4に中継されて基地局AP1にアクセスし、この基地局AP1からネットワークNWを通じて認証サーバASに接続され、またその逆の経路でASから無線端末MT7と通信する。

【0011】このような無線マルチホップネットワークでは、新規無線端末MTは認証前には基地局APまでの経路情報を保持していないので、認証要求をブロードキャストで送信する。この場合、新規MTの近隣の複数のMTが認証要求を受信し、それぞれがその認証要求を基地局に通じる次のMTへ中継する。この結果として、同じ認証処理が同時に発生することになる。

【0012】図54に無線マルチホップネットワークにおける認証時の問題を示す。無線端末MT9が新規MTの認証を装ってD o S攻撃をかけた場合、この無線端末MT9からブロードキャストで送り出される信号を図示では複数の無線端末MT5, MT6, MT7が同時に受信し、これらの無線端末がさらに他の無線端末を通じて複数の基地局AP # i, AP # jにアクセスし、これから認証サーバASに認証要求を同時に送信することになり、無線マルチホップネットワーク上に不正なパケットが流入し、他のパケットの転送が妨害されることになるのである。

【0013】本発明は、このような提案されている無線アクセスネットワーク、無線マルチホップネットワークにおいて、DoS攻撃に対する耐性に優れた技術を提供することを目的とする。

【0014】

【課題を解決するための手段】請求項1の発明は、無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセスネットワークにおいて、

A. 前記基地局は、前記事業者側ネットワークに新規に接続するときに基地局－認証サーバ間認証用パケットを送信して前記認証サーバと相互認証を行う処理機能、
 B. 前記無線端末は、当該無線アクセスネットワークに新規にアクセスするときに近隣にある基地局と相互認証を行い、認証成功後に無線端末－認証サーバ間認証用パケットを送信し、前記基地局は、前記無線端末との相互認証が成功したときに当該無線端末から送信されてきた前記無線端末－認証サーバ間認証用パケットの転送を許可し、前記認証サーバは、前記無線端末－認証サーバ間認証用パケットにより前記基地局を介して前記無線端末と相互認証を行う処理機能、

C. 前記無線端末、基地局、認証サーバそれぞれは、前記認証用パケットそれを送信し又は転送するときに送信元を示すパケット検査データを当該認証用パケットに添付する処理機能、

D. 前記無線端末、基地局、認証サーバそれぞれは、前記無線端末－認証サーバ間認証用パケットを受信したときに、それに添付されているパケット検査データを検査し、当該検査が失敗した場合はそれが添付されている認証用パケットを破棄する処理機能、

E. 前記認証サーバは認証した新規の基地局、新規の無線端末それとの情報を自装置に登録する処理機能を備えたものである。

【0015】請求項1の発明の無線アクセスネットワークでは、認証サーバ(AS)と基地局(AP)が相互認証を行うことで、事業者が一般ユーザの設置したAPの安全性を保障することが可能となる。新規無線端末(MT)がアクセスしたとき、最初にMT-AP間で相互認証することで互いが正当な装置であるか否かを確認することができ、APはこの相互認証が成功するまでは新規MTが送信したパケットを事業者側ネットワークに転送しないので、認証を装ったDoS攻撃を防止することができる。

【0016】MT-AP間の相互認証成功後にMT-AS間の相互認証及びこの認証用パケットのパケット検査(送信元確認)を行うことでASはどのAPにどのMTがアクセスしたかを正確に把握して管理することが可能となる。

【0017】請求項2の発明は、中継能力を持つ無線端

末と、この無線端末と無線通信する基地局と、この基地局と事業者側ネットワークを通じて接続される認証サーバとから構成される無線マルチホップネットワークにおいて、

A. 前記基地局は、新規に事業者側ネットワークに接続するときに前記認証サーバと基地局－認証サーバ間認証用パケットを用いて相互認証を行う処理機能、

B. 前記無線端末は、新規に当該無線マルチホップネットワークにアクセスするときに近隣の認証済みの無線端末又は基地局と無線端末間認証用パケットによって相互認証を行う処理機能、

C. 前記無線端末間の相互認証が成功した無線端末又は基地局が複数あれば、その中から1つの無線端末又は基地局を選択し、前記選択された無線端末又は基地局は、前記新規無線端末から送信された無線端末－認証サーバ間認証用パケットの転送を許可する処理機能、

D. 前記新規無線端末は、前記無線端末間の相互認証の成功後に、無線端末－認証サーバ間認証用パケットを用い、選択した無線端末又は基地局を経由して前記認証サーバと相互認証を行う処理機能、

E. 前記新規無線端末、選択された無線端末、基地局、認証サーバそれぞれは、前記無線端末－認証サーバ間認証用パケットを送信し又は転送するときに送信元を示すパケット検査データを当該認証用パケットに添付する処理機能、

F. 前記新規無線端末、選択された無線端末、基地局、認証サーバそれぞれは、前記認証用パケットそれを受信したときに、それに添付されているパケット検査データを検査し、当該検査が失敗した場合はそれが添付されている認証用パケットを破棄する処理機能、

G. 前記認証サーバは相互認証に成功した新規の基地局、新規の無線端末それとの情報を自装置に登録する処理機能を備えたものである。

【0018】請求項2の発明の無線マルチホップネットワークでは、新規無線端末(MT)が無線マルチホップネットワークにアクセスしたとき、最初に新規MT-近隣MT間で相互認証することで互いが正当な装置であるか否かを確認することができ、近隣のMTはこの相互認証が成功するまでは新規MTが送信したパケットを無線マルチホップネットワークに転送しないので、認証を装ったDoS攻撃を防止することができる。

【0019】また、相互認証の際にMT-AS(認証サーバ)間相互認証用パケットを中継させるMT又はAP(基地局)を1つ選択することで、同じ認証処理が同時に複数発生してしまうことを防止する。

【0020】さらに、MT-AP間の相互認証成功後にMT-AS間の相互認証及びこの認証用パケットのパケット検査(送信元確認)を行うことでASはどのAPにどのMTがアクセスしたかを正確に把握して管理することが可能となる。

【0021】請求項3の発明は、無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセシネットワークに用いられる無線端末であって、前記無線アクセシネットワークに新規にアクセスするときに、無線端末ー基地局間認証用パケットを送信して近隣の基地局と相互認証を行い、認証成功後に無線端末ー認証サーバ間認証用パケットを送信し、認証サーバとの間で相互認証を行う機能を備えたものである。

【0022】請求項3の発明の無線端末(MT)では、無線アクセシネットワークに新規に参入するときに基地局(AP)と相互認証を行い、その成功の後に認証サーバ(AS)と相互認証を行う機能を備えたことで、APに新規MTとの相互認証が成功するまで新規MTの送信したパケットを事業者側ネットワークに転送しない機能を持たせることによって、当該MTを用いなければAPとの通信、ひいては認証サーバ(AS)との通信ができない無線アクセシネットワークを構築することができ、認証を装ったDOS攻撃に耐性の強い無線アクセシネットワークの構築に寄与できる。

【0023】請求項4の発明は、請求項3の無線端末において、送信する無線端末ー認証サーバ間認証用パケットに送信元を示すパケット検査データを算出して添付する機能を備えたものであり、無線端末ー認証サーバ間認証用パケットにパケット検査データを添付することにより、受信先の基地局に送信元を明かすことができ、不正な攻撃のために用いられなくなる。

【0024】請求項5の発明は、請求項3又は4の無線端末において、前記無線端末ー基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、無線端末ー基地局間認証において正当な1つの基地局を選択し、当該基地局を通じて前記無線端末ー認証サーバ間認証用パケットを前記認証サーバに送信する機能を備えたものである。

【0025】請求項6の発明は、請求項5の無線端末において、前記無線端末ー基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、応答の早い基地局から優先的に選択して無線端末ー基地局間認証を実行する機能を備えたものである。

【0026】請求項7の発明は、請求項5の無線端末において、前記無線端末ー基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、応答信号の受信レベルの強い基地局から優先的に選択して無線端末ー基地局間認証を実行する機能を備えたものである。

【0027】請求項8の発明は、請求項5の無線端末において、前記無線端末ー基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、各基地局間との無線端末ー基地局間の認証手続きにおいて取得した情報に基づき、正当な基地局を選択する機能を備えたものである。

【0028】請求項5～8の発明の無線端末(MT)では、新規MTはMTーAP(基地局)間相互認証の際にMTーAS(認証サーバ)間相互認証用パケットを中継させるAP又はMTを所定のロジックにしたがって選択することで、同じ認証処理が同時に複数発生してしまうことを防止することができる。

【0029】請求項9の発明は、無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセシネットワーク又は無線マルチアクセシネットワークに用いられる認証サーバであって、新規にアクセスしてきた基地局と相互認証を実行し、認証が成功した基地局の情報を自装置に登録する機能と、無線端末ー認証サーバ間認証用パケットにパケット検査データを添付して基地局に送信し、基地局から送られてきた無線端末ー認証サーバ間認証用パケットに添付されているパケット検査データを検査し、検査が失敗した場合はそのパケットを破棄し、この検査が成功すれば無線端末との相互認証を実施し、相互認証に成功した無線端末の情報を自装置に登録する機能を備えたものである。

【0030】請求項9の発明の認証サーバ(AS)では、基地局(AP)と相互認証を行い、また新規無線端末(MT)とも相互認証を行い、しかも新規無線端末との相互認証の際に認証用パケットに添付されている送信元を示すパケット検査データを検査し、この検査が成功すれば相互認証を実施することになるので、不正なAPを排除し、正規のAPだけを管理することができ、またどのAPにどのMTがアクセスしたかをも正確に把握することが可能となる。

【0031】請求項10の発明は、請求項9の認証サーバにおいて、相互認証に成功した無線端末が別の基地局の通信エリアへ移動したとき、当該無線端末との新たな相互認証を実施し、認証が成功した後に当該無線端末の属していた旧基地局へその無線端末が移動したことを通知する機能を備えたものである。

【0032】請求項10の発明の認証サーバ(AS)では、自身の認証した無線端末(MT)の移動を管理し、MTがある基地局(AP)から別のAPへ移動した時、MTーAS間の相互認証が成功した後に、そのMTが属していた旧APへ当該MTが移動したことを通知することにより、APに一度は相互認証したがいまでは移動して通信できなくなったMTの記録をいつまでも保持させなくてよく、APにおけるMTの管理データを少なくでき、それだけ処理の高速化が図れる。

【0033】請求項11の発明は、無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセシネットワーク又は無線マルチホップネットワークにおいて用いられる基地局であって、新規に前記無線アクセシネットワーク又は無線マルチホップ

ネットワークに接続したときに、基地局－認証サーバ間認証用パケットを前記認証サーバに送信して相互認証を実行する機能を備えたものである。

【0034】請求項11の発明の基地局（AP）では、新規に無線アクセスネットワーク又は無線マルチホップネットワークに接続するときには必ず認証サーバと相互認証を実施するため、不正にAPを設置することを困難にし、事業者が一般ユーザの設置したAPの安全性を保障することが可能となる。

【0035】請求項12の発明は、請求項11の基地局において、新規の無線端末からの無線端末－基地局間認証要求に対して相互認証を行い、当該相互認証が成功したときに当該無線端末から送信されてきた無線端末－認証サーバ間認証用パケットに対して、それに添付されているパケット検査データを検査し、検査が失敗した場合はそのパケットを破棄し、当該検査が成功すれば、当該無線端末－認証サーバ間認証用パケットに自装置で算出したパケット検査データを添付して認証サーバに転送し、認証サーバから送信されてきた認証用パケットに示されている認証結果を参照して新規無線端末が送信したすべてのパケットの事業者側ネットワークへの転送を許可するか否かを判定する機能を備えたことを特徴とするものである。

【0036】請求項12の発明の基地局（AP）では、新規無線端末（MT）がアクセスしてきたとき、最初にMT－AP間で相互認証することでMTが正当な装置であるか否かを確認し、この相互認証が成功するまでは新規MTが送信したパケットを事業者側ネットワークに転送しないので、認証を装ったDOS攻撃を防止することができる。

【0037】請求項13の発明は、請求項11又は12の基地局において、相互認証に成功した無線端末それぞれの情報を自装置に登録する機能と、認証サーバから移動通知を受けて、該当する無線端末の登録情報を削除する機能とを備えたものであり、無線端末が他の基地局の通信エリアに移動した場合に、通信ができなくなってしまった無線端末の情報を削除することによって無線端末の管理のためのリソースを節約できる。

【0038】請求項14の発明は、中継能力を持つ無線端末と、この無線端末と無線通信する基地局と、この基地局と事業者側ネットワークを通じて接続される認証サーバとから構成される無線マルチホップネットワークにおいて用いられる無線端末であって、自装置が新規に無線マルチホップネットワークにアクセスするときには近隣の認証済みの他の無線端末又は基地局と相互認証を行い、複数の無線端末又は基地局と相互認証が成功した場合、正当な1つの無線端末又は基地局をプロキシ端末として選択し、当該プロキシ端末を介して認証サーバとの相互認証を実行する機能と、自装置が他の新規無線端末によって選択されたプロキシ端末である場合には、他の

新規無線端末から送信された新規無線端末－認証サーバ間認証用パケットをルート上の他の無線端末又は基地局に対して転送する機能とを備えたものである。

【0039】請求項14の発明の無線端末（MT）では、無線マルチホップネットワークに新規にアクセスするとき、最初に近隣MT又はAPとの間で相互認証する機能を備えたことで、当該MTが新規に無線マルチホップネットワークに参入する際には近隣のMT又はAPに正当な装置であるか否かを確認させ、近隣のMT又はAPはこの相互認証が成功するまでは当該MTが送信したパケットを無線マルチホップネットワークに転送しないので、認証を装ったDOS攻撃に対する耐性の高い無線マルチホップネットワークの構築に寄与できる。

【0040】請求項14の発明の無線端末（MT）ではまた、相互認証の際にMT－AS（認証サーバ）間相互認証用パケットを中継させるMT又はAP（基地局）を1つ選択する機能を備えたことで、同じ認証処理が同時に複数発生してしまうことを防止する。

【0041】請求項15の発明は、請求項14の無線端末において、自装置が新規に無線マルチホップネットワークにアクセスするときに、無線端末間認証用パケットを近隣の他の無線端末又は基地局に送信する機能と、自装置が新規無線端末である場合に、無線端末－認証サーバ間認証用パケットに送信元を示すパケット検査データを添付して送信する機能と、自装置が他の新規無線端末によって選択されたプロキシ端末である場合には、他の新規無線端末から送信された無線端末－認証サーバ間認証用パケットに対してパケット検査データを検査し、検査が失敗すればその認証用パケットを破棄し、当該検査が成功すれば当該認証用パケットに自装置で算出した送信元を示すパケット検査データを添付してルート上の他の無線端末又は基地局に対して転送する機能とを備えたものであり、どの基地局（AP）にどの無線端末（MT）がアクセスしたかを認証サーバに正確に把握することができる。

【0042】請求項16の発明は、請求項14又は15の無線端末において、基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局から応答を受けたとき、応答の早い基地局又は他の無線端末から優先的にプロキシ端末として選択する機能を備えたものである。

【0043】請求項17の発明は、請求項14又は15の無線端末において、基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局から応答を受けたとき、受信レベルの強い基地局又は他の無線端末から優先的にプロキシ端末として選択する機能を備えたものである。

【0044】請求項18の発明は、請求項14又は15の無線端末において、基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局か

ら応答を受けたとき、相互認証で取得した他の無線端末又は基地局の情報に基づいてプロキシ端末を選択する機能を備えたものである。

【0045】請求項16～18の発明の無線端末(MT)では、MT-Ap(基地局)間相互認証の際にMT-Ap(認証サーバ)間相互認証用パケットを中継させるAp又はMTとして最適なものを選択する機能を備えたことで、同じ認証処理が同時に複数発生してしまうことを防止することができる。

【0046】

【発明の実施の形態】以下、本発明の実施の形態を図に基づいて詳説する。

【0047】[第1の実施の形態] 図1は本発明の第1の実施の形態の無線アクセスマッシュワークの機能構成を示し、図2は認証サーバASの機能構成、図3は基地局Apの機能構成、図4は無線端末MTの機能構成を示している。この実施の形態の無線アクセスマッシュワークは、無線端末MT、この無線端末MTと無線通信する基地局Ap、この基地局Apと事業者側有線ネットワークNWを通じて接続される認証サーバASから構成される。

【0048】認証サーバASはソフトウェアとして、無線端末MTとの相互認証を実行する無線端末との認証機能101、認証した無線端末MTを、データベースを利用して管理する無線端末管理機能102、ネットワークNWのパケットを検査する有線区間パケット検査機能103、パケット判別機能104を備え、加えて、基地局との相互認証を実行する基地局との相互認証機能105、認証した基地局Apを、データベースを利用して管理する基地局管理機能106を備えている。

【0049】基地局Apはソフトウェアとして、認証サーバASと無線端末MT間の認証用パケットの転送を行う認証用パケット転送機能201、無線ネットワークのパケットを検査する無線区間パケット検査機能202、有線ネットワークNWのパケットを検査する有線区間パケット検査機能203、パケット判別機能204を備え、加えて、認証サーバASとの相互認証を実行する認証サーバとの相互認証機能206、無線端末MTとの相互認証を実行する無線端末との相互認証機能207、受信したパケットの転送可否を判断するパケット転送判断機能208、データベースを利用して無線端末MTを管理する無線端末管理機能209を備えている。

【0050】無線端末MTはソフトウェアとして、認証サーバASとの相互認証を実行する認証サーバとの相互認証機能301、無線ネットワークのパケットを検査する無線区間パケット検査機能302、パケット判別機能303を備え、加えて、基地局Apとの相互認証を実行する基地局との相互認証機能305を備えている。

【0051】次に、上記構成の第1の実施の形態の無線アクセスマッシュワークの動作について、説明する。

【0052】<基地局Ap-認証サーバAS間の相互認証>基地局Apは一般ユーザが設置し、この基地局Apから事業者の認証サーバASへのアクセス回線はそのユーザが契約したものとする。その基地局Apは設置したユーザだけでなく、他ユーザも使用することができる。他ユーザがその基地局Apを使用したとき、基地局Apを設置したユーザに対して事業者からペイバックが行われる。

【0053】ネットワークNWに一般ユーザが新規に基地局(Ap#kとする)を設置した時、この基地局Ap#kは事業者が管理する認証サーバASと認証を行う。認証シーケンスを図5、認証用パケットペイロードデータを図6に示す。また、Ap側から見た認証フローを図4に示し、AS側から見た認証フローを図8に示す。

【0054】初めに、図4のフローのステップS101で、基地局Ap#kは鍵生成情報KEap#kを計算し、その鍵生成情報を添付した認証要求を送信する。

【0055】図8のフローのステップS111で、その認証要求を受信した認証サーバASは鍵生成情報KEasを計算し、基地局の鍵生成情報KEap#kとこの認証サーバ側の鍵生成情報KEasからAp#k-AS間の共有鍵Kap#k-asを計算する(ステップS112)。認証サーバASはさらに乱数R1を計算し、鍵生成情報KEasと乱数R1を添付した認証要求応答をAp#kへ送信する(ステップS113)。

【0056】図4のフローのステップS102で、認証要求応答を受信した基地局Ap#kは、KEap#kとKEasからAp#k-AS間の共有鍵Kap#k-asを計算し(ステップS103)、R1、自装置の秘密鍵SKap#kを用いて署名データSigap#kを計算する(ステップS104)。基地局Ap#kはさらに乱数R2を計算し、R2、自装置の証明書Certap#k、そしてSigap#kを認証情報に添付してそのパケットを認証サーバASへ送信する(ステップS105)。

【0057】図8のフローのステップS114で基地局Ap#kから認証情報を受信した認証サーバASは、Certap#kを検査する(ステップS115)。もし検査が失敗した場合は、認証失敗を示す認証結果をAp#kへ送信する(ステップS117, S118)。Certap#kの検査が成功した場合は、さらにこのCertap#kからAp#kの公開鍵PKap#kを取り出し、このPKap#kを用いてSigap#kを検査する(ステップS115)。もし検査が失敗した場合にも認証失敗を示す認証結果をAp#kへ送信する(ステップS117, S118)。

【0058】ステップS115の検査が成功した場合は、認証サーバASは基地局Ap#kが正規のものであると判断し、R2、自装置の秘密鍵SKasを用いて署名データSigasを計算する(ステップS116)。

そして認証サーバASは、自装置の証明書Certasと署名データSigasを認証結果に添付し、そのパケットをAP#kへ送信する（ステップS118）。

【0059】図4のフローのステップS106で、認証サーバASから認証結果を受信した基地局AP#kは、受信したCertasを検査する。もし検査が失敗した場合は、最初から認証処理を開始する（ステップS107でNOに分岐）。検査が成功した場合にはさらに、CertasからASの公開鍵PKasを取り出し、このPKasを用いてSigasをも検査する。APは、この検査も成功した場合は、ASは事業者が設置した正規のASであると判断し、AP#k-AS間の相互認証が完了する。ステップS107でSigasの検査が失敗した場合にも、受信した認証結果を破棄し、最初から認証処理を開始する。

【0060】このようにして、認証サーバASが新規基地局APを認証すればデータベースに登録することで、事業者はユーザが設置したAPを把握し、他のユーザはそうしたAPを事業者が設置したものと同等の安全性を持つものとみなして使用することができる。

【0061】<無線端末MT-基地局AP間の相互認証>ある新規の無線端末MT#iがAP#kを介してネットワークNWにアクセスしようとしたとき、MT#iは初めにAP#kと認証を行う。AP#kはこの認証が成功するまでMT#iから送信されたパケットを事業者側ネットワークNWに転送しない。MT認証シーケンスを図9に、認証用パケットのペイロードデータを図10に示す。さらに、MT側から見た認証フローを図11に示し、AP側から見た認証フローを図12に示す。

【0062】初めに、図11のフローのステップS201で、無線端末MT#iは鍵生成情報KEmt#iを計算し、その鍵生成情報を添付した認証要求1を基地局AP#kへ送信する。

【0063】図12のフローのステップS211で、無線端末MT#iからの認証要求1を受信した基地局AP#kは、鍵生成情報KEap#kを計算し、無線端末側の鍵生成情報KEmt#iと当該基地局側の鍵生成情報KEap#kからMT#i-AP#k間の共有鍵Kmt#i-ap#kを計算する（ステップS212）。基地局AP#kはさらに乱数R1を計算し、鍵生成情報KEap#k、乱数R1を添付した認証要求応答1を無線端末MT#iへ送信する（ステップS213）。

【0064】図11のフローのステップS202で、基地局AP#kからの認証要求応答1を受信した無線端末MT#iは、自装置の鍵生成情報KEmt#iと基地局の鍵生成情報KEap#kからMT#i-AP#k間の共有鍵Kmt#i-ap#kを計算し（ステップS203）、さらに乱数R1、自装置の秘密鍵SKmt#iを用いて署名データSigm#iを計算する（ステップS204）。当該無線端末MT#iはさらに、乱数R2

を計算し、R2、自装置の証明書Certmt#i、署名データSigm#iを認証情報1に添付してそのパケットを基地局AP#kへ送信する（ステップS205）。

【0065】図12のフローのステップS214で、無線端末MT#iからの認証情報1を受信したAP#kは、Certmt#iを検査する（ステップS215）。もし検査が失敗した場合は、認証失敗を示す認証結果1をMT#iに送信する（ステップS219～S221）。検査が成功した場合はCertmt#iからMT#iの公開鍵PKmt#iを取り出す。基地局AP#kはMT#iの公開鍵PKmt#iを用いてSigm#iも検査する（ステップS215）。

【0066】基地局AP#kは、この検査が成功すれば無線端末MT#iが正規のMTであると判断し、乱数R2、自装置の秘密鍵SKap#kを用いて署名データSigm#kを計算する（ステップS216）。そして基地局AP#kは、自装置の証明書Certap#kと署名データSigm#kを認証結果1に添付し、そのパケットを無線端末MT#iへ送信する（ステップS217）。また基地局AP#kは、無線端末MT#iの認証が成功した時点で、MT#iから送信される認証2用パケットの認証サーバASへの転送を許可する（ステップS218）。ステップS215で無線端末MT#iの署名データSigm#iの検査が失敗した場合にも、認証失敗を示す認証結果1をMT#iに送信し（ステップS219、S220）、無線端末MT#iから送信される認証2用パケットの認証サーバASへの転送を不許可にする（ステップS221）。

【0067】図11のフローのステップS206で、基地局AP#kからの認証結果1を受信したMT#iは、基地局の証明書Certap#kを検査する（ステップS207）。もし検査が失敗した場合は、認証1を最初から開始する（ステップS207でNOに分岐）。検査が正しい場合はこのCertap#kから基地局AP#kの公開鍵PKap#kを取り出す。さらに無線端末MT#iは、取り出した公開鍵PKap#kを用いて基地局AP#kの署名データSigm#kを検査する。この検査も正しい場合は、この基地局AP#kが事業者の認めた正規のAPであると判断し、MT#i-AP#k間の相互認証が完了する（ステップS207でYESに分岐）。もし検査が失敗した場合にも、認証1を最初から開始する（ステップS207でNOに分岐）。

【0068】このようにして、基地局AP#kは無線端末MT#iの認証に成功するまで事業者側ネットワークに当該無線端末MT#iによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバASへの攻撃を防止することができる。同時に、基地局APを所有するユーザのアクセス回線が不正に利用されることも防止することができる。

【0069】<無線端末MT#i-認証サーバAS間の相互認証>上記の無線端末MT#i-基地局AP#k間の相互認証が成功したら、無線端末MT#iは当該基地局AP#kを介して認証サーバASとの認証を行う。無線端末MT#i側から見た認証フローを図13に示し、認証サーバAS側から見た認証フローを図14に示す。さらに、基地局AP#K側から見た認証フローを図15、図16に示す。そしてパケットペイロードデータは図10に示すものである。

【0070】図13のフローのステップS231で、初めに、無線端末MT#iはシーケンス番号SQNを生成し、そのSQNと共有鍵Kmt#i-ap#kを用いて送信元を示すパケット検査データPCVを計算する。無線端末MT#iは、これらのSQN、PCVを付加した認証要求2を基地局AP#kへ送信する（ステップS232）。

【0071】図15のフローのステップS241で、無線端末MT#iからの認証要求2を受信した基地局AP#kは、PCVをSQN、Kmt#i-ap#kを用いて検査する。もし検査が失敗した場合は受信した認証要求2を破棄する。検査が成功した場合は受信パケット中のSQNと共有鍵Kap#k-asを用いてPCVを計算する（ステップS242）。基地局AP#kは、この新PCVを生成すると、元のPCVを廃棄し、新しいPCVを付加した認証要求2を認証サーバASへ送信する（ステップS243）。

【0072】図14のフローのステップS251で、基地局AP#kから認証要求2を受信した認証サーバASは、受信したPCVをシーケンス番号SQN、共有鍵Kap#k-asを用いて検査する（ステップS252）。もし検査が失敗した場合は受信した認証要求2を破棄する。検査が成功した場合は乱数R3を計算する。認証サーバASはさらに、シーケンス番号SQNを生成し、そのSQNと共有鍵Kap#k-asを用いてPCVを計算し（ステップS253）、乱数R3とこれらのSQN、PCVを付加した認証要求応答2を基地局AP#kへ送信する（ステップS254）。

【0073】図15のフローのステップS241で、認証サーバASから認証要求応答2を受信した基地局AP#kは、シーケンス番号SQNと共有鍵Kap#k-asを用いてPCVを検査する。この検査の結果が正しければ、基地局AP#kはSQNと共有鍵Kmt#i-ap#kを用いて新しいPCVを計算する（ステップS242）。基地局AP#kは新しいPCVを生成すると旧いPCVを廃棄し、新しいPCVを付加した認証要求応答2を無線端末MT#iへ送信する（ステップS243）。

【0074】図13のフローのステップS233で、認証要求応答2を受信した無線端末MT#iは、PCVをSQN、Kmt#i-ap#kを用いて検査する（ステ

ップS234）。もし検査が失敗した場合は、受信した認証要求応答2を破棄する。無線端末MT#iは、PCVの検査が成功した場合は、乱数R3、秘密鍵SKmt#iを用いて署名データSigmt#iを計算する（ステップS235）。さらに無線端末MT#iは、乱数R4を計算し、この乱数R4、自装置の証明書Certmt#i、署名データSigmt#i及び上記と同様の手順で計算したPCVを認証情報2に付加してそのパケットを基地局AP#kへ送信する（ステップS236、S237）。

【0075】図15のフローのステップS241で、無線端末MT#iからの認証情報2を受信した基地局AP#kはPCVを検査し、正しければ上記と同様の手順で計算したPCVを付加して認証情報2を認証サーバASへ送信する（ステップS242、S243）。

【0076】図14のフローのステップS255で、基地局AP#kからの認証情報2を受信したASは、PCVを検査する（ステップS256）。もし検査が失敗した場合は、受信した認証情報2を破棄する。検査が成功した場合は署名データCertmt#iを検査する。もし検査が失敗した場合は認証失敗を示す認証結果2に新しいSQN、上記と同様の手順で計算したPCVを付加して基地局AP#kへ送信する（ステップS261～S263）。ステップS257で署名データCertmt#iの検査が成功した場合は、この署名データCertmt#iから無線端末MT#iの公開鍵PKmt#iを取り出す。認証サーバASはさらに、この公開鍵PKmt#iを用いて署名データSigmt#iを検査する（ステップS257）。

【0077】認証サーバASはステップS257でMT#iの検査も成功すれば、無線端末MT#iが正規のMTであると判断し、乱数R4、自装置の秘密鍵SKasを用いて署名データSigasを計算する（ステップS258）。認証サーバASはさらに、自装置の証明書CertasとSigas、上記と同様の手順で計算したPCVを認証結果2に付加し、そのパケットを基地局AP#kへ送信する（ステップS259、S260）。この検査が失敗した場合にも、認証失敗を示す認証結果2に新しいSQN、PCV付加して基地局AP#kへ送信する（ステップS261～S263）。

【0078】図16のフローのステップS271で、認証サーバASから認証結果2を受信した基地局AP#kは、PCVを検査し、結果が正しければ新しいPCVを付加して認証結果2をMT#iへ送信する（ステップS272～S274）。この認証結果2が認証成功を示している場合は、基地局AP#kはこの時点でMT#iから送信されるデータパケットの事業者側ネットワークへの転送を許可する（ステップS275）。

【0079】ステップS271で受信した認証結果2が認証失敗を示している場合、基地局AP#kは無線端末

MT#i から送信されるデータパケットの事業者側ネットワークへの転送を許可しない（ステップS272, S276～S278）。

【0080】図13のフローのステップS238で認証結果2を受信した無線端末MT#iは、PCVを検査する（ステップS239）。もし検査が失敗した場合は、無線端末MT#iは認証情報2を再送する（ステップS236, S237）。検査が成功した場合、無線端末MT#iはCertasを検査する（ステップS240）。もしこの検査が失敗した場合、無線端末MT#iは最初から認証2を開始する。Certasの検査が成功した場合、無線端末MT#iはCertasから認証サーバASの公開鍵PKasを取り出し、この公開鍵PKasを用いて署名データSigasを検査する。もしこの検査が失敗した場合にも、最初から認証2を開始する（ステップS240でNOに分岐）。この署名データSigasの検査も成功した場合、無線端末MT#iは認証サーバASが事業者の認めた正規のASであると判断し、MT#i～AS間の相互認証が完了する（ステップS240）。

【0081】このように第1の実施の形態の無線アクセスマッシュネットワークでは、認証2用パケットにパケット検査データ(PCV)を付加することで、認証サーバAPは正規の無線端末MTから送信されたパケットであることを確認し、認証2を利用した攻撃を防止することができる。また、認証サーバASは、無線端末MTから送信された認証2用パケットが正規の基地局APを経由して送信されたことを確認できる。さらに、基地局APが無線端末MTを認証した後に認証サーバASが無線端末MTを認証することで、事業者はどの基地局APにどの無線端末MTがアクセスしているかを把握でき、かつ基地局APが不正に無線端末MTのアクセスを申告して事業者からペイバックを受けるような不正サービス利用や不正な課金情報の申告を防止することができる。

【0082】〔第2の実施の形態〕次に、本発明の無線アクセスマッシュネットワークの第2の実施の形態について、説明する。第2の実施の形態のネットワークの特徴は、図17に示すような状況、つまり、新規無線端末MTと通信できるエリアに基地局AP#1とAP#kとが存在し、これらのいずれとも認証手続きのために通信できる状況で、新規無線端末MTがMT～AS間相互認証用パケットを中継させる基地局として適切なもの（ここではAP#k）を選択することにより、同じ認証処理が同時に複数発生してしまうことを防止する機能を備えた点にある。

【0083】これを実現するために、無線端末MTは図18、図19に示す機能構成を備えている。すなわち、図1に示した第1の実施の形態の機能構成に加えて、基地局選択機能306を備えていて、この基地局選択機能306が、最初に受信した基地局を中継のために基地局

に選択することにより同じ認証処理が同時に複数発生してしまうことを防止する。

【0084】次に、第2の実施の形態の無線アクセスマッシュネットワークの動作を、図20の無線端末認証シーケンス、図21の無線端末の基地局AP選択処理を含めたAP認証フローを用いて説明する。

【0085】ネットワークNWに一般ユーザが新規に基地局AP#kを設置した時、AP#kは事業者が管理する認証サーバASと認証を行うが、この手続きは第1の実施の形態と共通であり、図5の認証シーケンス、図6の認証用パケットペイロードデータ、図7及び図8のAP～AS間認証フローの通りである。

【0086】ある無線端末MT#1が基地局APを介してネットワークにアクセスしようとしたとき、MT#1は初めにAPと認証を行う。基地局APはこの認証が成功するまで無線端末MT#1から送信されたパケットを事業者側ネットワークNWに転送しない。MT認証シーケンスを図20に示す。なお、第2の実施の形態で用いるMT認証用パケットのペイロードデータは、第1の実施の形態と同様に図10に示すものである。また、AP側から見たMT～AP間認証フローは図12に、MT～AS間認証フローは図13及び図14に、中継となる基地局AP#k側のMT～AS間認証フローは図15及び図16にそれぞれ示した第1の実施の形態のものと同様である。ただし、第2の実施の形態の場合、MT側のMT～AP間認証フローが図21に示したものに変更される点が異なる。

【0087】図21に示したMT側から見たMT～AP間認証フローのステップS301で、ある無線端末MT#iがネットワークにアクセスしようとしたとき、鍵生成情報KEmt#iを計算し、その鍵生成情報を添付した認証要求1を基地局APへブロードキャストで送信する。

【0088】第1の実施の形態と同様に、図12のフローのステップS211で、無線端末MT#1から認証要求1を受信したAP#kは、鍵生成情報KEap#kを計算し、さらにMT#i～AP#k間の共有鍵Kmt#i～ap#kを計算する（ステップS212）。さらに基地局AP#kは、乱数R1を計算し、KEap#k、R1を添付した認証要求応答1をMT#iへ送信する（ステップS213）。

【0089】図17に示した状況では基地局AP#1も同じ無線端末MT#iからの認証要求1を受信するので、同様にして鍵生成情報KEap#1を計算し、MT#i～AP#1間の共有鍵Kmt#i～ap#1を計算する（ステップS212）。基地局AP#1はさらに、乱数R1'を計算し、KEap#1、R1'を添付した認証要求応答1をMT#iへ基地局AP#kと同様に送信する（ステップS213）。

【0090】図21のフローのステップS302～S3

04で、無線端末MT#iは予め基地局選択機能306に組み込まれたロジック、つまり、最初に受信した認証要求応答1に対して処理を行うというロジックに基づき、2番目以降に受信した認証処理応答1はそれよりも先に受信された基地局の認証処理応答1が選択された場合に廃棄する。ここでは、最初に基地局AP#kからの認証処理応答1を受信し、基地局AP#1からの認証処理応答1はそれに遅れて受信したものとする。

【0091】基地局AP#kからの認証要求応答1を最初に受信したMT#iは、ステップS305で、第1の実施の形態と同様に自装置の鍵生成情報KEmt#iと基地局AP#kの鍵生成情報KEap#kからMT#i-AP#k間の共有鍵Kmt#i-ap#kを計算する。そして、乱数R1、自装置の秘密鍵SKmt#iを用いて署名データSigmt#iを計算する（ステップS306）。続いて、無線端末MT#iは乱数R2を計算し、R2、自装置の証明書Certmt#i、Sigmt#iを認証情報1に添付してそのパケットを選択した基地局AP#kへ送信する（ステップS307）。

【0092】図12のフローのステップS214で、無線端末MT#iからの認証情報1を受信した基地局AP#kは、以降、第1の実施の形態と同様の処理を実行し、基地局MT#iが正規のMTであると判断すれば、認証結果1をMT#iへ送信し（ステップS215～S217）、またMT#iの認証が成功した時点でMT#iから送信される認証2用パケットのASへの転送を許可する（ステップS218）。一方、もしMTの検査に失敗した場合は、認証失敗を示す認証結果1をMT#iへ送信し、MT#iから送信される認証2用パケットのASへの転送を不許可にする（ステップS219～S221）。

【0093】図21のフローのステップS308で基地局AP#kから認証結果1を受信した無線端末MT#iは基地局AP#kの証明書Certap#kを検査する（ステップS309）。この検査が失敗した場合は、最初から認証1を開始する。そしてこの場合、最初に受信した基地局AP#kからの認証要求応答1のパケットを廃棄し、2番目に受信した基地局AP#1からの認証要求応答1に対して認証処理を行うことになる。つまり、2度目の認証でも最初にAP#k、2番目のAP#1からの応答を受信したとすれば、ステップS303、S311で最初のAP#kのパケットは破棄する。そしてステップS304で2番目に受信したAP#1の認証要求応答1について、認証処理を実施するのである。

【0094】ステップS309において、基地局AP#kの証明書Certap#kの検査が成功した場合は、無線端末MT#iはCertap#kから基地局AP#kの公開鍵PKap#kを取り出し、このPKap#kを用いてSigap#kを検査し、この検査も成功すれば基地局AP#kが事業者の設置した正規のAPである

と判断し、MT#i-AP#k間の相互認証が完了する。この検査が失敗した場合にも、最初から認証1を開始する。そしてこの場合にも、2番目に受信した基地局AP#1からの認証要求応答1に対して同様に認証処理を行うことになる。

【0095】上記の認証1が成功したら、無線端末MT#iは選択した基地局AP#kを介して認証サーバASと認証を行う。このMT-AS間の認証手続きは、第1の実施の形態と同様であり、MT側のMT-AS間認証フローは図13に、AP側のMT-AS間認証フローは図14に、中継となる基地局AP#k側のMT-AS間認証フローは図15及び図16にそれぞれ示したものである。

【0096】この第2の実施の形態の無線アクセスマルチネットワークによれば、第1の実施の形態と同様、基地局AP#kが無線端末MT#iの認証が成功するまで事業者側ネットワークにMT#iによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバASへの攻撃を防止することができ、また、基地局APを所有するユーザのアクセス回線が不正に利用されることも防止することができる。さらに第2の実施の形態の場合、正規の基地局APを1つ選択することで同一の認証2用パケットが認証サーバASへ同時に送信されることを防止できる。

【0097】【第3の実施の形態】次に、本発明の第3の実施の形態の無線アクセスマルチネットワークについて、説明する。第3の実施の形態の無線アクセスマルチネットワークは、機能構成は第2の実施の形態と同様であるが、図17に示した状況、つまり、新規無線端末MT#iが複数の基地局AP#1、AP#kから同時に、あるいは相前後して認証要求応答1を受信した場合に、受信信号レベルが最も高い基地局（ここではAP#kとする）を選択し、以降の認証手続きを実行する点に特徴を有する。図22は、第3の実施の形態において、無線端末MTの基地局選択処理を含むAP認証フローを示している。その他の処理は全て第2の実施の形態と共通である。

【0098】無線端末MTの備える機能構成は、図18に示す第2の実施の形態と同様である。ただし、基地局選択機能306が、受信レベルが最大である基地局を選ぶことによって同じ認証処理が同時に複数発生してしまうことを防止する点で第2の実施の形態とは異なる。

【0099】次に、第3の実施の形態の無線アクセスマルチネットワークの動作を、図20の無線端末認証シーケンス、図22の無線端末の基地局AP選択処理を含めたAP認証フローを用いて説明する。

【0100】ネットワークに一般ユーザが新規に基地局AP#kを設置した時、AP#kは事業者が管理する認証サーバASと認証を行うが、この手続きは第1、第2の実施の形態と共通であり、図5の認証シーケンス、図6の認証用パケットペイロードデータ、図7及び図8の

A P - A S間認証フローの通りである。

【0101】ある無線端末MT#iが基地局APを介してネットワークにアクセスしようとしたとき、MT#1は初めにAPと認証を行う。基地局APはこの認証が成功するまで無線端末MT#1から送信されたパケットを事業者側ネットワークNWに転送しない。なお、第3の実施の形態で用いるMT認証用パケットのペイロードデータは、第1の実施の形態と同様に図10に示すものである。また、AP側から見たMT-A P間認証フローは図12に、MT-A S間認証フローは図13及び図14に、中継となる基地局AP#k側のMT-A S間認証フローは図15及び図16にそれぞれ示した第1、第2の実施の形態のものと同様である。

【0102】図22に示したMT側から見たMT-A P間認証フローのステップS301で、ある無線端末MT#iがネットワークにアクセスしようとしたとき、鍵生成情報KEmt#iを計算し、その鍵生成情報を添付した認証要求1を基地局APへブロードキャストで送信する。

【0103】第1の実施の形態と同様に、図12のフローのステップS211で、無線端末MT#1から認証要求1を受信したAP#kは、鍵生成情報KEap#kを計算し、さらにMT#i-A P#k間の共有鍵Kmt#i-ap#kを計算する（ステップS212）。さらに基地局AP#kは、乱数R1を計算し、KEap#k、R3を添付した認証要求応答1をMT#iへ送信する（ステップS213）。

【0104】図17に示した状況では基地局AP#1も同じ無線端末MT#iからの認証要求1を受信するので、同様にして鍵生成情報KEap#1を計算し、MT#i-A P#1間の共有鍵Kmt#i-ap#1を計算する（ステップS212）。基地局AP#1はさらに、乱数R1'を計算し、KEap#1、R1'を添付した認証要求応答1をMT#iへ基地局AP#kと同様に送信する（ステップS213）。

【0105】図22のフローのステップS302～304'で、無線端末MT#iは予め基地局選択機能306に組み込まれたロジック、つまり、送信後の所定時間内に受信した認証要求応答1の信号レベルが一番高い基地局を選択するというロジックに基づき基地局を選択し、それ以外の認証処理応答1は廃棄する（ステップS304'、S312）。したがって、最初の認証処理応答で、基地局AP#1とAP#kとから所定時間内に認証要求応答1を受信した無線端末MT#iは、それらの認証要求応答1の受信レベルを測定し、測定レベルの高い基地局AP#kからの認証要求応答1に対して処理を行い、AP#1の認証要求応答1のパケットは廃棄することになる。

【0106】図22のフローのステップS304'で基地局AP#kからの認証要求応答1を選択したMT#i

は、ステップS305で、第1、第2の実施の形態と同様に、自装置の鍵生成情報KEmt#iと基地局AP#kの鍵生成情報KEap#kからMT#i-A P#k間の共有鍵Kmt#i-ap#kを計算する。そして、乱数R1、自装置の秘密鍵SKmt#iを用いて署名データSigmt#iを計算する（ステップS306）。続いて、無線端末MT#iは乱数R2を計算し、R2、自装置の証明書Certmt#i、Sigmt#iを認証情報1に添付してそのパケットを選択した基地局AP#kへ送信する（ステップS307）。

【0107】図12のフローのステップS214で、無線端末MT#iからの認証情報1を受信した基地局AP#kは、以降、第1、第2の実施の形態と同様の処理を実行し、基地局MT#iが正規のMTであると判断すれば、認証結果1をMT#iへ送信し（ステップS215～S217）、またMT#iの認証が成功した時点でMT#iから送信される認証2用パケットのA Sへの転送を許可する（ステップS218）。一方、もしMTの検査に失敗した場合は、認証失敗を示す認証結果1をMT#iへ送信し、MT#iから送信される認証2用パケットのA Sへの転送を不許可にする（ステップS219～S221）。

【0108】図22のフローのステップS308で基地局AP#kから認証結果1を受信した無線端末MT#iは、基地局AP#kの証明書Certap#kを検査する（ステップS309）。この検査が失敗した場合は、ステップS301に戻り、最初から認証1を開始する。

【0109】ステップS309において、基地局AP#kの証明書Certap#kの検査が成功した場合は、無線端末MT#iはCertap#kから基地局AP#kの公開鍵PKap#kを取り出し、このPKap#kを用いてSgap#kを検査し、この検査も成功すれば基地局AP#kが事業者の認めた正規のAPであると判断し、MT#i-A P#k間の相互認証が完了する。この検査が失敗した場合にも、最初から認証1を開始する。

【0110】ステップS309で最初から認証1を繰り返す判定に至った場合、無線端末MT#iはブロードキャストで認証要求1を再度送信する（ステップS301）。これに対して、第1回目と同様に基地局AP#k、AP#1が認証要求応答1を返信してきたとし、しかも基地局AP#kの受信レベルの方が基地局AP#1の受信レベルよりも高かったとする。

【0111】この場合、ステップS302でMT#iは基地局AP#kを最初に選択するが、これに対してステップS303で、第1回目の判定でNGと判断された基地局であると判定してそのパケットを破棄する（ステップS303、S311）。そして次の基地局AP#1の認証要求応答1を採用し、ステップS304'で他に受信レベルがAP#1よりも高いものがないと判定す

ば、この基地局AP#1の認証要求応答1に対してステップS305以降の処理を実施する。なお、ステップS305以降の処理は、図21のフローに示した第2の実施の形態と同様である。

【0112】この第3の実施の形態の無線アクセスマッシュトワークによれば、第2の実施の形態と同様、基地局AP#kが無線端末MT#iの認証が成功するまで事業者側ネットワークにMT#iによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバASへの攻撃を防止することができ、また、基地局APを所有するユーザのアクセス回線が不正に利用されることも防止することができる。さらに第3の実施の形態の場合、正規の基地局APを1つ選択することで同一の認証用パケットが認証サーバASへ送信されることを防止できる。加えて、信号受信レベルの高い基地局を選択することで無線通信の信頼性を高めることができる。

【0113】【第4の実施の形態】第4の実施の形態の無線アクセスマッシュトワークは、機能構成は第2の実施の形態と同様であるが、図17に示した状況、つまり、新規無線端末MT#iが複数の基地局AP#1, AP#kから同時に、あるいは相前後して認証要求応答1を受信した場合に、受信信号レベルが最も高い基地局（ここではAP#kとする）を選択し、以降の認証手続きを実行する点に特徴を有する。図23は、第4の実施の形態において、無線端末MTの基地局選択処理を含むAP認証フローを示している。その他の処理は全て第2、第3の実施の形態と共通である。

【0114】無線端末MTの備える機能構成は、図18に示す第2、第3の実施の形態と同様である。ただし、基地局選択機能306が、帯域使用状況を受信した複数の基地局それについて確認し、最も帯域に空きがある基地局から優先的に選択して認証要求応答1に対して処理を行うことによって、同じ認証処理が同時に複数発生してしまうことを防止する点で第2、第3の実施の形態とは異なる。

【0115】次に、第4の実施の形態の無線アクセスマッシュトワークの動作を、図20の無線端末認証シーケンス、図23の無線端末の基地局AP選択処理を含めたAP認証フローを用いて説明する。

【0116】ネットワークに一般ユーザが新規に基地局AP#kを設置した時、AP#kは事業者が管理する認証サーバASと認証を行うが、この手続きは第1、第2の実施の形態と共通であり、図5の認証シーケンス、図6の認証用パケットペイロードデータ、図7及び図8のAP-AS間認証フローの通りである。

【0117】ある無線端末MT#iが基地局APを介してネットワークにアクセスしようとしたとき、MT#iは初めにAPと認証を行う。基地局APはこの認証が成功するまで無線端末MT#iから送信されたパケットを事業者側ネットワークNWに転送しない。なお、第4の

実施の形態で用いるMT認証用パケットのペイロードデータも、第1の実施の形態と同様に図10に示すものである。また、AP側から見たMT-AP間認証フローは図12に、MT-AS間認証フローは図13及び図14に、中継となる基地局AP#k側のMT-AS間認証フローは図15及び図16にそれぞれ示した第1、第2の実施の形態のものと同様である。

【0118】図23に示したMT側から見たMT-AP間認証フローのステップS301で、ある無線端末MT#iがネットワークにアクセスしようとしたとき、鍵生成情報KEmt#iを計算し、その鍵生成情報を添付した認証要求1を基地局APへブロードキャストで送信する。

【0119】第1の実施の形態と同様に、図12のフローのステップS211で、無線端末MT#1から認証要求1を受信したAP#kは、鍵生成情報KEap#kを計算し、さらにMT#i-AP#k間の共有鍵Kmt#i-ap#kを計算する（ステップS212）。さらに基地局AP#kは、乱数R1を計算し、KEap#k、R3を添付した認証要求応答1をMT#iへ送信する（ステップS213）。

【0120】図17に示した状況では基地局AP#1も同じ無線端末MT#iからの認証要求1を受信するので、同様にして鍵生成情報KEap#1を計算し、MT#i-AP#1間の共有鍵Kmt#i-ap#1を計算する（ステップS212）。基地局AP#1はさらに、乱数R1'を計算し、KEap#1、R1'を添付した認証要求応答1をMT#iへ基地局AP#kと同様に送信する（ステップS213）。

【0121】図23のフローのステップS302～304”で、無線端末MT#iは予め基地局選択機能306に組み込まれたロジック、つまり、送信後の所定時間内に送信してきた基地局の中で最も帯域に空きがある基地局を選択するというロジックに基づき基地局を選択し、それ以外の認証処理応答1は廃棄する（ステップS304”，S312）。したがって、最初の認証処理応答で、基地局AP#1とAP#kとから所定時間内に認証要求応答1を受信した無線端末MT#iは、それらの基地局の帯域の空き状況を確認し、帯域の空きが大きい基地局AP#kからの認証要求応答1に対して処理を行い、AP#1の認証要求応答1のパケットは廃棄することになる。

【0122】図23のフローのステップS304”で基地局AP#kからの認証要求応答1を選択したMT#iは、ステップS305で、第1、第2の実施の形態と同様に、自装置の鍵生成情報KEmt#iと基地局AP#kの鍵生成情報KEap#kからMT#i-AP#k間の共有鍵Kmt#i-ap#kを計算する。そして、乱数R1、自装置の秘密鍵SKmt#iを用いて署名データSigmt#iを計算する（ステップS306）。続

いて、無線端末MT#iは乱数R2を計算し、R2、自装置の証明書Certmt#i、Sigmt#iを認証情報1に添付してそのパケットを選択した基地局AP#kへ送信する(ステップS307)。

【0123】図12のフローのステップS214で、無線端末MT#iからの認証情報1を受信した基地局AP#kは、以降、第1、第2の実施の形態と同様の処理を実行し、基地局MT#iが正規のMTであると判断すれば、認証結果1をMT#iへ送信し(ステップS215～S217)、またMT#iの認証が成功した時点でMT#iから送信される認証2用パケットのASへの転送を許可する(ステップS218)。一方、もしMTの検査に失敗した場合は、認証失敗を示す認証結果1をMT#iへ送信し、MT#iから送信される認証2用パケットのASへの転送を不許可にする(ステップS219～S221)。

【0124】図23のフローのステップS308で基地局AP#kから認証結果1を受信した無線端末MT#iは、基地局AP#kの証明書Certcap#kを検査する(ステップS309)。この検査が失敗した場合は、ステップS301に戻り、最初から認証1を開始する。

【0125】ステップS309において、基地局AP#kの証明書Certcap#kの検査が成功した場合は、無線端末MT#iはCertcap#kから基地局AP#kの公開鍵PKap#kを取り出し、このPKap#kを用いてSigcap#kを検査し、この検査も成功すれば基地局AP#kが事業者の認めた正規のAPであると判断し、MT#i～AP#k間の相互認証が完了する。この検査が失敗した場合にも、最初から認証1を開始する。

【0126】ステップS309で最初から認証1を繰り返す判定に至った場合、無線端末MT#iはプロードキャストで認証要求1を再度送信する(ステップS301)。これに対して、第1回目と同様に基地局AP#k、AP#1が認証要求応答1を返信してきたとし、しかも第2回目にも基地局AP#kの方がap#1よりも使用帯域の空きが大きかったとする。

【0127】この場合、ステップS302でMT#iは基地局AP#kを最初に選択するが、これに対してステップS303で、第1回目の判定でNGと判断された基地局であると判定してそのパケットを破棄する(ステップS303、S311)。そして次の基地局AP#1の認証要求応答1を採用し、ステップS304”で他に候補となる基地局がないと判定すれば、この基地局AP#1の認証要求応答1に対してステップS305以降の処理を実施する。なお、ステップS305以降の処理は、図21のフローに示した第2の実施の形態の処理と同様である。

【0128】この第4の実施の形態の無線アクセスネットワークによれば、第2の実施の形態と同様、基地局A

P#kが無線端末MT#iの認証が成功するまで事業者側ネットワークにMT#iによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバASへの攻撃を防止することができ、また、基地局APを所有するユーザのアクセス回線が不正に利用されることも防止することができる。さらに第4の実施の形態の場合、正規の基地局APを1つ選択することで同一の認証2用パケットが認証サーバASへ送信されることを防止できる。加えて、使用帯域の空きが大きい基地局を選択することで無線通信の応答速度を高めることができる。

【0129】[第5の実施の形態] 次に、本発明の第5の実施の形態の無線アクセスネットワークについて、説明する。第5の実施の形態の無線アクセスネットワークは、機能構成は第2の実施の形態と同様であるが、図17に示した状況、つまり、新規無線端末MT#iが複数の基地局AP#1、AP#kから同時に、あるいは相前後して認証要求応答1を受信した場合に、そのすべてを一旦保持しておき、応答が早い基地局から順に認証1の処理を実施し、認証1が成功した基地局を選択し、以降の認証手続きを実行する点に特徴を有する。図24は、第5の実施の形態において、無線端末MTの基地局選択処理を含むAP認証フローを示している。その他の処理は全て第2の実施の形態と共通である。

【0130】無線端末MTの備える機能構成は、図18に示す第2の実施の形態と同様である。ただし、基地局選択機能306が、複数の基地局から認証要求応答1を受信した場合に、そのすべてを一旦保持しておき、応答が早い基地局から順に認証1の処理を実施し、認証1が成功した基地局を選択することにより同じ認証処理が同時に複数発生してしまうことを防止する点で第2の実施の形態とは異なる。

【0131】次に、第5の実施の形態の無線アクセスネットワークの動作を、図20の無線端末認証シーケンス、図24の無線端末の基地局AP選択処理を含めたAP認証フローを用いて説明する。

【0132】ネットワークに一般ユーザが新規に基地局AP#kを設置した時、AP#kは事業者が管理する認証サーバASと認証を行うが、この手続きは第1、第2の実施の形態と共にあり、図5の認証シーケンス、図6の認証用パケットペイロードデータ、図7及び図8のAP～AS間認証フローの通りである。

【0133】ある無線端末MT#iが基地局APを介してネットワークにアクセスしようとしたとき、MT#1は初めにAPと認証を行う。基地局APはこの認証が成功するまで無線端末MT#1から送信されたパケットを事業者側ネットワークNWに転送しない。なお、第5の実施の形態で用いるMT認証用パケットのペイロードデータは、第1の実施の形態と同様に図10に示すものである。また、AP側から見たMT～AP間認証フローは

図12に、MT-A S間認証フローは図13及び図14に、中継となる基地局AP#k側のMT-A S間認証フローは図15及び図16にそれぞれ示した第1、第2の実施の形態のものと同様である。

【0134】図24に示したMT側から見たMT-AP間認証フローのステップS401で、ある無線端末MT#iがネットワークにアクセスしようとしたとき、鍵生成情報KEmt#iを計算し、その鍵生成情報を添付した認証要求1を基地局APへブロードキャストで送信する。

【0135】第1の実施の形態と同様に、図12のフローのステップS211で、無線端末MT#1から認証要求1を受信したAP#kは、鍵生成情報KEap#kを計算し、さらにMT#i-AP#k間の共有鍵Kmt#i-ap#kを計算する(ステップS212)。さらに基地局AP#kは、乱数R1を計算し、KEap#k、R1を添付した認証要求応答1をMT#iへ送信する(ステップS213)。

【0136】図17に示した状況では基地局AP#1も同じ無線端末MT#iからの認証要求1を受信するので、同様にして鍵生成情報KEap#1を計算し、MT#i-AP#1間の共有鍵Kmt#i-ap#1を計算する(ステップS212)。基地局AP#1はさらに、乱数R1'を計算し、KEap#1、R1'を添付した認証要求応答1をMT#iへ基地局AP#kと同様に送信する(ステップS213)。

【0137】図24のフローのステップS402、S403で、無線端末MT#iは予め基地局選択機能306に組み込まれたロジック、つまり、送信後の所定時間内に受信した認証要求応答1のうち最先に受信した基地局を選択するというロジックに基づき基地局を選択し、それ以外の認証処理応答1に対する認証処理は保留にする。ここでは、基地局AP#kからの認証処理応答1が最先であったとして説明する。

【0138】基地局AP#1とAP#kとから所定時間内に認証要求応答1を受信した無線端末MT#iは、最先に応答してきた基地局AP#kからの認証要求応答1に対して処理を行う(ステップS402～S404)。他の受信した基地局AP#1からの認証処理応答1は、それよりも先に応答した基地局について認証1が成功するまでは保持されるが、先に応答した基地局が選択された時点で廃棄することになる。

【0139】図24のフローのステップS404で基地局AP#kからの認証要求応答1を選択したMT#iは、ステップS405で、第1、第2の実施の形態と同様に、自装置の鍵生成情報KEmt#iと基地局AP#kの鍵生成情報KEap#kからMT#i-AP#k間の共有鍵Kmt#i-ap#kを計算する。そして、乱数R1、自装置の秘密鍵SKmt#iを用いて署名データSgmt#iを計算する(ステップS406)。続

いて、無線端末MT#iは乱数R2を計算し、R2、自装置の証明書Certmt#i、Sgmt#iを認証情報1に添付してそのパケットを選択した基地局AP#kへ送信する(ステップS407)。

【0140】図12のフローのステップS214で、無線端末MT#iからの認証情報1を受信した基地局AP#kは、以降、第1、第2の実施の形態と同様の処理を実行し、基地局MT#iが正規のMTであると判断すれば、認証結果1をMT#iへ送信し(ステップS215～S217)、またMT#iの認証が成功した時点でMT#iから送信される認証2用パケットのASへの転送を許可する(ステップS218)。一方、もしMTの検査に失敗した場合は、認証失敗を示す認証結果1をMT#iへ送信し、MT#iから送信される認証2用パケットのASへの転送を不許可にする(ステップS219～S221)。

【0141】図24のフローのステップS408で基地局AP#kから認証結果1を受信した無線端末MT#iは基地局AP#kの証明書Certap#kを検査する(ステップS409)。この検査が失敗した場合は、当該パケットを破棄し(ステップS411)、他の基地局からの認証要求応答1を受信しているかどうか判断する(ステップS412)。

【0142】ステップS412で、他の基地局からの認証要求応答1が残っている場合にはステップS404に戻り、残っている認証要求応答1のうち応答が最も早かった基地局を選択し、ステップS405以降の処理を繰り返す。図17の状況では、最初に基地局AP#1が選択されることになるが、基地局AP#kの認証が不成功であれば、続いて応答してきた基地局AP#1について、ステップS405以降の処理が実施されることになる。なお、ステップS412において、他の基地局からの認証要求応答1が残っていない場合には、ステップS401に戻り、最初から認証1を開始する。

【0143】ステップS409において、基地局AP#kの証明書Certap#kの検査が成功した場合は、無線端末MT#iはCertap#kから基地局AP#kの公開鍵PKap#kを取り出し、このPKap#kを用いてSgapt#kを検査し、この検査も成功すれば基地局AP#kが事業者の認めた正規のAPであると判断し、MT#i-AP#k間の相互認証が完了する。この検査が失敗した場合にも、ステップS411、S412を実行し、2番目に応答してきた基地局AP#1からの認証要求応答1に対して同様に認証処理を行う。

【0144】上記の認証1が成功したら、無線端末MT#iは選択した基地局AP#kを介して認証サーバASと認証を行う。このMT-A S間の認証手続きは、第1、第2の実施の形態と同様であり、MT側のMT-A S間認証フローは図13に、AP側のMT-A S間認証フローは図14に、中継となる基地局AP#k側のMT

-AS間認証フローは図15及び図16にそれぞれ示したものである。

【0145】この第5の実施の形態の無線アクセスネットワークによれば、第1の実施の形態と同様、基地局AP#kが無線端末MT#iの認証が成功するまで事業者側ネットワークにMT#iによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバASへの攻撃を防止することができ、また、基地局APを所有するユーザのアクセス回線が不正に利用されることも防止することができる。さらに第5の実施の形態の場合、正規の基地局APを1つ選択することで同一の認証2用パケットが認証サーバASへ送信されることを防止できる。加えて、最先に応答した基地局から優先的に選択することで無線通信の応答速度を速めることができ、複数の基地局からの応答を無線端末側で一旦保持しておいて応答の時間的に早かったものから優先して認証処理を実施するので、第3の実施の形態の場合よりも通信処理が迅速化できる。

【0146】【第6の実施の形態】次に、本発明の第6の実施の形態の無線アクセスネットワークについて、説明する。第6の実施の形態の無線アクセスネットワークは、機能構成は第2の実施の形態と同様であるが、図17に示した状況、つまり、新規無線端末MT#iが複数の基地局AP#1, AP#kから同時に、あるいは相前後して認証要求応答1を受信した場合に、そのすべてを一旦保持しておく、応答信号の受信レベルが高い基地局から順に認証1の処理を実施し、認証1が成功した基地局を選択し、以降の認証手続きを実行する点に特徴を有する。図25は、第6の実施の形態において、無線端末MTの基地局選択処理を含むAP認証フローを示している。その他の処理は全て第2の実施の形態と共通である。

【0147】無線端末MTの備える機能構成は、図18に示す第2の実施の形態と同様である。ただし、基地局選択機能306が、複数の基地局から認証要求応答1を受信した場合に、そのすべてを一旦保持しておく、応答信号の受信レベルが高い基地局から順に認証1の処理を実施し、認証1が成功した基地局を選択することにより同じ認証処理が同時に複数発生してしまうことを防止する点で第2の実施の形態とは異なる。

【0148】次に、第6の実施の形態の無線アクセスネットワークの動作を、図20の無線端末認証シーケンス、図25の無線端末の基地局AP選択処理を含めたAP認証フローを用いて説明する。

【0149】ネットワークに一般ユーザが新規に基地局AP#kを設置した時、AP#kは事業者が管理する認証サーバASと認証を行うが、この手続きは第1、第2の実施の形態と共通であり、図5の認証シーケンス、図6の認証用パケットペイロードデータ、図7及び図8のAP-AS間認証フローの通りである。

【0150】ある無線端末MT#iが基地局APを介してネットワークにアクセスしようとしたとき、MT#1は初めにAPと認証を行う。基地局APはこの認証が成功するまで無線端末MT#1から送信されたパケットを事業者側ネットワークNWに転送しない。なお、第6の実施の形態で用いるMT認証用パケットのペイロードデータは、第1の実施の形態と同様に図10に示すものである。また、AP側から見たMT-AP間認証フローは図12に、MT-AS間認証フローは図13及び図14に、中継となる基地局AP#k側のMT-AS間認証フローは図15及び図16にそれぞれ示した第1、第2の実施の形態のものと同様である。

【0151】図25に示したMT側から見たMT-AP間認証フローのステップS401で、ある無線端末MT#iがネットワークにアクセスしようとしたとき、鍵生成情報KEmt#iを計算し、その鍵生成情報を添付した認証要求1を基地局APへブロードキャストで送信する。

【0152】第1の実施の形態と同様に、図12のフローのステップS211で、無線端末MT#1から認証要求1を受信したAP#kは、鍵生成情報KEap#kを計算し、さらにMT#i-AP#k間の共有鍵Kmt#i-ap#kを計算する(ステップS212)。さらに基地局AP#kは、乱数R1を計算し、KEap#k、R1を添付した認証要求応答1をMT#iへ送信する(ステップS213)。

【0153】図17に示した状況では基地局AP#1も同じ無線端末MT#iからの認証要求1を受信するので、同様にして鍵生成情報KEap#1を計算し、MT#i-AP#1間の共有鍵Kmt#i-ap#1を計算する(ステップS212)。基地局AP#1はさらに、乱数R1'を計算し、KEap#1、R1'を添付した認証要求応答1をMT#iへ基地局AP#kと同様に送信する(ステップS213)。

【0154】図25のフローのステップS402、S403で、無線端末MT#iは予め基地局選択機能306に組み込まれたロジック、つまり、送信後の所定時間内に受信した認証要求応答1のうち受信レベルが最も高い基地局を選択するというロジックに基づき基地局を選択し、それ以外の認証処理応答1に対する認証処理は保留にする。ここでは、基地局AP#kからの認証処理応答1の受信レベルが最高であったとして説明する。

【0155】基地局AP#1とAP#kとから所定時間内に認証要求応答1を受信した無線端末MT#iは、受信レベルが高い方の基地局AP#kからの認証要求応答1に対して処理を行う(ステップS402～S404')。他の受信した基地局AP#1からの認証処理応答1は、それよりも受信レベルが高い他の基地局について認証1が成功するまでは保持されるが、受信レベルが高い他の基地局が選択された時点で廃棄することにな

る。

【0156】図25のフローのステップS404'で基地局AP#kからの認証要求応答1を選択したMT#iは、ステップS405で、第1、第2の実施の形態と同様に、自装置の鍵生成情報KEmt#iと基地局AP#kの鍵生成情報KEap#kからMT#i-AP#k間の共有鍵Kmt#i-ap#kを計算する。そして、乱数R1、自装置の秘密鍵SKmt#iを用いて署名データSigmt#iを計算する（ステップS406）。続いて、無線端末MT#iは乱数R2を計算し、R2、自装置の証明書Certmt#i、Sigmt#iを認証情報1に添付してそのパケットを選択した基地局AP#kへ送信する（ステップS407）。

【0157】図12のフローのステップS214で、無線端末MT#iからの認証情報1を受信した基地局AP#kは、以降、第1、第2の実施の形態と同様の処理を実行し、基地局MT#iが正規のMTであると判断すれば、認証結果1をMT#iへ送信し（ステップS215～S217）、またMT#iの認証が成功した時点でMT#iから送信される認証2用パケットのASへの転送を許可する（ステップS218）。一方、もしMTの検査に失敗した場合は、認証失敗を示す認証結果1をMT#iへ送信し、MT#iから送信される認証2用パケットのASへの転送を不許可にする（ステップS219～S221）。

【0158】図25のフローのステップS408で基地局AP#kから認証結果1を受信した無線端末MT#iは基地局AP#kの証明書Certap#kを検査する（ステップS409）。この検査が失敗した場合は、当該パケットを破棄し（ステップS411）、他の基地局からの認証要求応答1を受信しているかどうか判断する（ステップS412）。

【0159】ステップS412で、他の基地局からの認証要求応答1が残っている場合にはステップS404'に戻り、残っている認証要求応答1のうち応答信号の受信レベルが最も高い基地局を選択し、ステップS405以降の処理を繰り返す。図17の状況では、最初に基地局AP#1が選択されることになるが、基地局AP#kの認証が不成功であれば、次の受信レベルが高い基地局AP#1について、ステップS405以降の処理が実施されることになる。なお、ステップS412において、他の基地局からの認証要求応答1が残っていない場合には、すべてのパケットを破棄し、ステップS401に戻り、最初から認証1を開始する。

【0160】ステップS409において、基地局AP#kの証明書Certap#kの検査が成功した場合は、無線端末MT#iはCertap#kから基地局AP#kの公開鍵PKap#kを取り出し、このPKap#kを用いてSiga#kを検査し、この検査も成功すれば基地局AP#kが事業者の認めた正規のAPであると

判断し、MT#i-AP#k間の相互認証が完了する。この検査が失敗した場合にも、ステップS411、S412を実行し、応答信号の受信レベルが2番目に高い基地局AP#1からの認証要求応答1に対して同様に認証処理を行う。

【0161】上記の認証1が成功したら、無線端末MT#iは選択した基地局AP#kを介して認証サーバASと認証を行う。このMT-AS間の認証手続きは、第1、第2の実施の形態と同様であり、MT側のMT-AS間認証フローは図13に、AP側のMT-AS間認証フローは図14に、中継となる基地局AP#k側のMT-AS間認証フローは図15及び図16にそれぞれ示したものである。

【0162】この第6の実施の形態の無線アクセスマルチネットワークによれば、第1の実施の形態と同様、基地局AP#kが無線端末MT#iの認証が成功するまで事業者側ネットワークにMT#iによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバASへの攻撃を防止することができ、また、基地局APを所有するユーザーのアクセス回線が不正に利用されることも防止することができる。さらに第6の実施の形態の場合、正規の基地局APを1つ選択することで同一の認証2用パケットが認証サーバASへ送信されることを防ぐことができる。加えて、応答信号の受信レベルが高い基地局から優先的に選択することで無線通信の信頼性を高めることができ、しかも複数の基地局からの応答を無線端末側で一旦保持しておいて応答信号の受信レベルの高いものから優先して認証処理を実施するので、第2の実施の形態の場合よりも通信処理が迅速化できる。

【0163】[第7の実施の形態] 次に、本発明の第7の実施の形態の無線アクセスマルチネットワークについて、説明する。第7の実施の形態の無線アクセスマルチネットワークは、機能構成は第2の実施の形態と同様であるが、図17に示した状況、つまり、新規無線端末MT#iが複数の基地局AP#1、AP#kから同時に、あるいは相前後して認証要求応答1を受信した場合に、そのすべてを一旦保持しておき、各基地局の帯域使用状況を確認し、帯域の空きが大きい基地局から順に認証1の処理を実施し、認証1が成功した基地局を選択し、以降の認証手続きを実行する点に特徴を有する。図26は、第7の実施の形態において、無線端末MTの基地局選択処理を含むAP認証フローを示している。その他の処理は全て第2の実施の形態と共通である。

【0164】無線端末MTの備える機能構成は、図18に示す第2の実施の形態と同様である。ただし、基地局選択機能306が、複数の基地局から認証要求応答1を受信した場合に、そのすべてを一旦保持しておき、帯域の空きが大きい基地局から順に認証1の処理を実施し、認証1が成功した基地局を選択することにより同じ認証処理が同時に複数発生してしまうことを防止する点で第

2の実施の形態とは異なる。

【0165】次に、第7の実施の形態の無線アクセスネットワークの動作を、図20の無線端末認証シーケンス、図26の無線端末の基地局AP選択処理を含めたAP認証フローを用いて説明する。

【0166】ネットワークに一般ユーザが新規に基地局AP#kを設置した時、AP#kは事業者が管理する認証サーバASと認証を行うが、この手続きは第1、第2の実施の形態と共通であり、図5の認証シーケンス、図6の認証用パケットペイロードデータ、図7及び図8のAP-AS間認証フローの通りである。

【0167】ある無線端末MT#iが基地局APを介してネットワークにアクセスしようとしたとき、MT#iは初めにAPと認証を行う。基地局APはこの認証が成功するまで無線端末MT#1から送信されたパケットを事業者側ネットワークNWに転送しない。なお、第7の実施の形態で用いるMT認証用パケットのペイロードデータは、第1の実施の形態と同様に図10に示すものである。また、AP側から見たMT-AP間認証フローは図12に、MT-AS間認証フローは図13及び図14に、中継となる基地局AP#k側のMT-AS間認証フローは図15及び図16にそれぞれ示した第1、第2の実施の形態のものと同様である。

【0168】図26に示したMT側から見たMT-AP間認証フローのステップS401で、ある無線端末MT#iがネットワークにアクセスしようとしたとき、鍵生成情報KEmt#iを計算し、その鍵生成情報を添付した認証要求1を基地局APへブロードキャストで送信する。

【0169】第1の実施の形態と同様に、図12のフローのステップS211で、無線端末MT#1から認証要求1を受信したAP#kは、鍵生成情報KEap#kを計算し、さらにMT#i-AP#k間の共有鍵Kmt#i-ap#kを計算する（ステップS212）。さらに基地局AP#kは、乱数R1を計算し、KEap#k、R1を添付した認証要求応答1をMT#iへ送信する（ステップS213）。

【0170】図17に示した状況では基地局AP#1も同じ無線端末MT#iからの認証要求1を受信するので、同様にして鍵生成情報KEap#1を計算し、MT#i-AP#1間の共有鍵Kmt#i-ap#1を計算する（ステップS212）。基地局AP#1はさらに、乱数R1'を計算し、KEap#1、R1'を添付した認証要求応答1をMT#iへ基地局AP#kと同様に送信する（ステップS213）。

【0171】図26のフローのステップS402、S403で、無線端末MT#iは予め基地局選択機能306に組み込まれたロジック、つまり、送信後の所定時間内に受信した認証要求応答1のうち帶域の空きが最も大きい基地局を選択するというロジックに基づき基地局を選

択し、それ以外の認証処理応答1に対する認証処理は保留にする。ここでは、基地局AP#kの帶域の空きが最も大きいとして説明する。

【0172】基地局AP#1とAP#kとから所定時間内に認証要求応答1を受信した無線端末MT#iは、帶域の空きが大きい方の基地局AP#kからの認証要求応答1に対して処理を行う（ステップS402～S404）。他の受信した基地局AP#1からの認証処理応答1は、帶域の空きがそれよりも大きい他の基地局について認証1が成功するまでは保持されるが、他の基地局が選択された時点で廃棄することになる。

【0173】図26のフローのステップS404で基地局AP#kからの認証要求応答1を選択したMT#iは、ステップS405で、第1、第2の実施の形態と同様に、自装置の鍵生成情報KEmt#iと基地局AP#kの鍵生成情報KEap#kからMT#i-AP#k間の共有鍵Kmt#i-ap#kを計算する。そして、乱数R1、自装置の秘密鍵SKmt#iを用いて署名データSigmt#iを計算する（ステップS406）。続いて、無線端末MT#iは乱数R2を計算し、R2、自装置の証明書Certmt#i、Sigmt#iを認証情報1に添付してそのパケットを選択した基地局AP#kへ送信する（ステップS407）。

【0174】図12のフローのステップS214で、無線端末MT#iからの認証情報1を受信した基地局AP#kは、以降、第1、第2の実施の形態と同様の処理を実行し、基地局MT#iが正規のMTであると判断すれば、認証結果1をMT#iへ送信し（ステップS215～S217）、またMT#iの認証が成功した時点でMT#iから送信される認証2用パケットのASへの転送を許可する（ステップS218）。一方、もしMTの検査に失敗した場合は、認証失敗を示す認証結果1をMT#iへ送信し、MT#iから送信される認証2用パケットのASへの転送を不許可にする（ステップS219～S221）。

【0175】図26のフローのステップS408で基地局AP#kから認証結果1を受信した無線端末MT#iは基地局AP#kの証明書Certap#kを検査する（ステップS409）。この検査が失敗した場合は、当該パケットを破棄し（ステップS411）、他の基地局からの認証要求応答1を受信しているかどうか判断する（ステップS412）。

【0176】ステップS412で、他の基地局からの認証要求応答1が残っている場合にはステップS404に戻り、残っている認証要求応答1のうち帶域の空きが最も大きい基地局のものを選択し、ステップS405以降の処理を繰り返す。図17の状況では、最初に基地局AP#1が選択されることになるが、基地局AP#kの認証が不成功であれば、次には基地局AP#1について、ステップS405以降の処理が実施されることにな

る。なお、ステップS412において、他の基地局からの認証要求応答1が残っていない場合には、すべてのパケットを破棄し、ステップS401に戻り、最初から認証1を開始する。

【0177】ステップS409において、基地局AP#kの証明書Certap#kの検査が成功した場合は、無線端末MT#iはCertap#kから基地局AP#kの公開鍵PKap#kを取り出し、このPKap#kを用いてSigaP#kを検査し、この検査も成功すれば基地局AP#kが事業者の認めた正規のAPであると判断し、MT#i—AP#k間の相互認証が完了する。この検査が失敗した場合にも、ステップS411、S412を実行し、帯域の空きが2番目に大きい基地局AP#1からの認証要求応答1に対して同様に認証処理を行う。

【0178】上記の認証1が成功したら、無線端末MT#iは選択した基地局AP#kを介して認証サーバASと認証を行う。このMT—AS間の認証手続きは、第1、第2の実施の形態と同様であり、MT側のMT—AS間認証フローは図13に、AP側のMT—AS間認証フローは図14に、中継となる基地局AP#k側のMT—AS間認証フローは図15及び図16にそれぞれ示したものである。

【0179】この第7の実施の形態の無線アクセスマルチホップネットワークによれば、第1の実施の形態と同様、基地局AP#kが無線端末MT#iの認証が成功するまで事業者側ネットワークにMT#iによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバASへの攻撃を防止することができ、また、基地局APを所有するユーザのアクセス回線が不正に利用されることも防止することができる。さらに第7の実施の形態の場合、正規の基地局APを1つ選択することで同一の認証2用パケットが認証サーバASへ送信されることを防止できる。加えて、使用帯域の空きが大きい基地局から優先的に選択することで無線通信の応答処理速度を高めることができ、しかも複数の基地局からの応答を無線端末側で一旦保持しておいて帯域の空きが大きいものから優先して認証処理を実施するので、第4の実施の形態の場合よりも通信処理が迅速化できる。

【0180】【第8の実施の形態】次に、本発明の第8の実施の形態の無線アクセスマルチホップネットワークについて、図27～図32を用いて説明する。第8の実施の形態のシステムは、認証サーバASが経路となる無線端末と基地局の識別子を自装置のデータベースに登録して管理する機能を備えたことを特徴とする。この認証サーバASは、図27、図29に示す機能構成であり、図1に示した第1の実施の形態の機能構成に加えて、無線端末移動管理機能107を備えている。これに対応する基地局MTは、図28、図30に示す機能構成であり、図1に示した第1の実施の形態の機能構成に加えて、リソース開

放機能210を備えている。

【0181】認証サーバASによる無線端末及び基地局の管理機能は次のように実行される。図31はリソース開放シーケンス、図32はこのとき使用されるパケットフォーマットを示している。また、MT登録確認フローは図33に示している。

【0182】第1～第7の実施の形態のいずれかの無線アクセスマルチホップネットワークで、新規無線端末MT#iと認証サーバASと間の相互認証が成功した後、図33のフローに示すように、認証サーバASはその新規無線端末MT#iと、無線端末—認証サーバ間認証用パケットの中継を行った基地局AP1、AP2のそれぞれの識別子ID（MACアドレスを利用するのが好ましいが、本システムで新規に設定するIDであってもよい）を対データベースに登録し、管理する（ステップS501）。

【0183】また認証サーバASは、この登録時に、新規無線端末MT#iの識別子IDがすでにデータベースに登録されていないかを確認する（ステップS502）。もしすでに登録されている場合は、対となる基地局AP1に対して新規無線端末MT#iが別の基地局AP2に移動したことを示すリソース開放通知を送信する（ステップS503）。

【0184】リソース開放通知を受信した基地局AP1は、リソース開放通知中の無線端末MTの識別子を参照し、対応するリソースを開放し、リソース完了を認証サーバASに送信する。

【0185】これにより、第8の実施の形態の無線アクセスマルチホップネットワークでは、認証サーバASが、自身の認証した無線端末MT#iの移動を管理し、無線端末がある基地局AP1から別の基地局AP2へ移動した時、無線端末—認証サーバ間の相互認証が成功した後に、その無線端末が属していた旧基地局AP1へ当該無線端末MT#iが移動したことを通知することにより、基地局が一度は相互認証したがいまでは移動して通信できなくなつた無線端末MT#iの記録をいつまでも保持していくなくともよく、基地局における無線端末の管理データを少なくでき、それだけ処理の高速化が図れる。

【0186】【第9の実施の形態】本発明の第9の実施の形態の無線マルチホップネットワークについて、説明する。図34は本発明の第9の実施の形態の無線マルチホップネットワークの機能構成を示し、図35は認証サーバASの機能構成、図36は基地局MTの機能構成、図37は無線端末MTの機能構成を示している。第9の実施の形態の無線マルチホップネットワークは、パケット中継機能を付加的に備えた無線端末MT、パケット中継機能を備え、無線端末MTと無線通信する基地局AP、この基地局APと事業者側有線ネットワークNWを通じて接続される認証サーバASから構成される。

【0187】この無線マルチホップネットワークは、図38に示したように、例えば、無線端末MT9は、他の

無線端末MT3, MT2に中継されて基地局AP1にアクセスし、この基地局AP1からネットワークNWを通じて認証サーバASに接続され、またその逆の径路でASから無線端末MT9と通信する。

【0188】このため、図34、図35に示すように、認証サーバASはソフトウェアとして、無線端末MTとの相互認証を実行する無線端末との認証機能101、認証した無線端末MTを、データベースを利用して管理する無線端末管理機能102、ネットワークNWのパケットを検査する有線区間パケット検査機能103、パケット判別を行うパケット判別機能104を備え、加えて、基地局との相互認証を実行する基地局との相互認証機能105、認証した基地局APを、データベースを利用して管理する基地局管理機能106を備えている。

【0189】図34、図36に示すように、基地局APはソフトウェアとして、認証サーバAS-無線端末MT間の認証用パケットの転送を行う認証用パケット転送機能201、無線ネットワークのパケットを検査する無線区間パケット検査機能202、有線ネットワークNWのパケットを検査する有線区間パケット検査機能203、パケット判別を行うパケット判別機能204、パケット中継を行うパケット中継機能205を備え、加えて、認証サーバASとの相互認証を実行する認証サーバとの相互認証機能206、無線端末MTとの相互認証を実行する無線端末との相互認証機能207、受信したパケットの転送可否を判断するパケット転送判断機能208、認証した無線端末を、データベースによって管理する無線端末管理機能209、無線端末選択機能211を備えている。

【0190】図34、図37に示すように、無線端末MTはソフトウェアとして、認証サーバASとの相互認証を実行する認証サーバとの相互認証機能301、無線ネットワークのパケットを検査する無線区間パケット検査機能302、パケット判別を行うパケット判別機能303、他の無線端末からのパケットを中継するパケット中継機能304、他の無線端末又は基地局との相互認証を実行する無線端末との相互認証機能307、複数の無線端末又は基地局の1つをプロキシ端末として選択する無線端末選択機能308、プロキシ端末として選択された場合に認証用パケットを転送する認証用パケット転送機能309を備えている。

【0191】次に、上記構成の第9の実施の形態の無線マルチホップネットワークの動作について、説明する。図34及び図38に示す無線マルチホップネットワークにおいても、基地局APは事業者または一般ユーザが設置する。そして本ネットワークの場合、無線端末MTは近くの基地局だけでなく近くの無線端末に中継させて事業者ネットワークNWに送信することができる。また、このネットワークを実現するため、各無線端末MTは、他の無線端末MTから受信したパケット又は基地局APか

ら受信したパケットを、宛先のルート上にある隣接するMT又はAPへ転送することができる。

【0192】<認証サーバAS-基地局AP間の相互認証>ネットワークに一般ユーザが新規に基地局AP1を設置した時、基地局AP1は事業者が管理する認証サーバASと認証を行う。この認証シーケンスは第1の実施の形態と同様に図5に示すものであり、認証用パケットペイロードデータは図6に示すものである。また、認証フローも第1の実施の形態と同様で、図7及び図8に示すものとなる。ただし、基地局APの識別番号が、ここでは#k=1であり、AP#kに代えてAP1を用いる。

【0193】初めに図7のフローのステップS101で、基地局AP1は鍵生成情報KEap1を計算し、その鍵生成情報を添付した認証要求を送信する。

【0194】図8のフローのステップS111で、基地局AP1からの認証要求を受信した認証サーバASは、鍵生成情報KEasを計算し、KEap1とKEasからAP1-AS間の共有鍵Kap1-asを計算する（ステップS112）。認証サーバASはさらに、乱数R1を計算し、KEas、R1を添付した認証要求応答を基地局AP1へ送信する（ステップS113）。

【0195】図7のフローのステップS102で、認証サーバASからの認証要求応答を受信した基地局AP1は、自装置の鍵生成情報KEap1と認証サーバASの鍵生成情報KEasからAP1-AS間の共有鍵Kap1-asを計算し、乱数R1と自装置の秘密鍵SKap1を用いて署名データSigap1を計算する（ステップS104）。基地局AP1はさらに乱数R2を計算し、このR2、自装置の証明書Certap1、そしてSigap1を認証情報に添付してそのパケットを認証サーバASへ送信する（ステップS105）。

【0196】図8のフローのステップS114で、基地局AP1からの認証情報を受信した認証サーバASは、添付されているCertap1を検査する。もし検査が失敗した場合は、認証失敗を示す認証結果をAP1へ送信する（ステップS115, S117, S118）。検査が成功した場合は、Certap1からAP1の公開鍵PKap1を取り出し、さらにこのPKap1を用いてさらに基地局AP1の種名データSigap1を検査する。もしこの検査が失敗した場合にも、認証失敗を示す認証結果をAP1へ送信する（ステップS115, S117, S118）。

【0197】そしてこの検査も成功した場合は、基地局AP1は正規の基地局であると判断し、ステップS115でYESに分岐し、乱数R2、自装置の秘密鍵SKasを用いて署名データSigasを計算する（ステップS116）。認証サーバASはさらに、自装置の証明書Certasと署名データSigasを認証結果に添付し、そのパケットを基地局AP1へ送信する（ステップ

S118)。

【0198】図7のフローのステップS106で、認証サーバASからの認証結果を受信した基地局AP1は、添付されている認証サーバの署名データCertasを検査する。もし検査が失敗した場合は、最初から認証処理を開始する(ステップS107でNOに分岐)。この検査が成功した場合は、認証サーバの証明書Certasから認証サーバASの公開鍵PKasを取り出す。基地局AP1はさらに、取り出した公開鍵PKasを用いて認証サーバの署名データSigasを検査する。もし検査が失敗した場合にも、受信した認証結果を破棄し、最初から認証処理を開始する(ステップS107でNOに分岐)。検査が成功した場合は、認証サーバASは事業者が設置した正規の認証サーバであると判断し、AP1-AS間の相互認証が完了する(ステップS107でYESに分岐)。

【0199】このようにして認証サーバASが新規の基地局AP1を認証することで事業者はユーザが設置したAPを把握し、ユーザはそうしたAPを事業者が設置したものと同等の安全性を持つとみなして使用することができるようになる。

【0200】<無線端末MT-MT間の相互認証>図38に示したネットワークで、無線端末MT9がネットワークNWに初めてアクセスするとき、近隣の無線端末MT又は基地局APから認証を受ける。無線端末MT9の近隣にあるプロキシ端末となる無線端末MTあるいは基地局APは、MT9から送信されたパケットを、認証1が成功するまで自装置より先に転送しない。無線端末MT9の認証シーケンスを図39に示し、認証用パケットのペイロードデータを図40に示す。

【0201】なお、以下では、無線端末MT9の近隣には無線端末MT3、MT4、MT8が存在するが、無線端末MT9は無線端末選択機能308によりMT3を選択し、このMT3を最初に中継させ(プロキシ端末とする)、MT3-MT2-AP1のルートで認証サーバASと相互認証手続きを行うようになるものとして説明する。

【0202】図41の無線端末MT9から見た認証フローにおける最初のステップS601で、無線端末MT9は乱数R1を生成し、R1を付加した認証要求1をブロードキャストで送信する。図38の状況ではこの認証要求1は上述したように無線端末MT3、MT4、MT8によって同時に受信される。

【0203】図42のフローのステップS611で、無線端末MT9からの認証要求1を受信した無線端末MT3は、乱数R2を生成し、自装置の秘密鍵SKmt3と乱数R1を用いて署名データSigmt3を計算する(ステップS612)。無線端末MT3は統一して、乱数R2、Sigmt3、自装置の証明書Certmt3を付加した認証要求応答1を無線端末MT9に送信する

(ステップS613)。同様に、無線端末MT9からの認証要求1を受信したMT4、MT8それぞれも認証要求応答1をMT9に送信する。

【0204】図41のフローのステップS602で、複数の無線端末MT3、MT4、MT8からの認証要求応答1を受信した無線端末MT9は、それぞれに添付された証明書(Certmt3、Certmt4、Certmt8)を検査する。検査が失敗した場合は、受信した認証要求応答を破棄する。検査が成功した場合は、その証明書から公開鍵(PKmt3、PKmt4、PKmt8)を取り出し、その公開鍵を用いてそれぞれの署名データ(Sigmt3、Sigmt4、Sigmt8)を検査する(ステップS603)。

【0205】検査が成功した中継MTが1つもない場合には、受信した認証要求応答1を破棄し、最初に戻る(ステップS604でNOに分岐)。

【0206】検査が成功した中継MTが1つもある場合には、ステップS604でYESに分岐する。そして検査に成功した中継MTが複数ある場合、その中に基地局APが含まれていれば基地局を優先的にプロキシ(Proxy)端末として選択し、検査に成功したのが無線端末ばかりであれば、新規の無線端末MT9は基地局AP1、AP2までのルート情報RInfoを調べ、APまでのホップ数が最も小さい1つのMTを選択する。さらに、候補が複数ある場合にはランダムに候補の中から1つの中継MTを選択する(ステップS605)。ここでは無線端末MT3が選択されたものとする。なお、候補が複数ある場合に、受信信号レベルが最高の無線端末、あるいは最初に受信した無線端末を選択するようにしてもよい。こうして選択された無線端末MT3は新規無線端末MT9のProxyMTとなる。

【0207】無線端末MT9は統一して、乱数R2と自装置の秘密鍵SKmt9を用いて署名データSigmt9を計算し、これらR2、Sigmt9、自装置の証明書Certmt9を付加した認証情報1をProxyMT(ここではMT3)へ送信する(ステップS606、S607)。

【0208】無線端末MT9により選択された無線端末MT3は、図42のフローのステップS614でMT9からの認証情報1を受信すると、新規無線端末MT9の証明書Certmt9を検査する。もし検査が失敗した場合は、認証失敗を示す認証結果1をMT9へ送信する(ステップS615、S618-S620)。

【0209】検査が成功した場合は、Certmt9から公開鍵PKmt9を取り出し、この公開鍵PKmt9を用いて無線端末MT9の署名データSigmt9を検査する。もしこの検査が失敗した場合にも、無線端末MT3は認証失敗を示す認証結果1を無線端末MT9へ送信し、MT3はMT9から送信される認証2用パケットのAPへの転送を不許可にする(ステップS615、S

618～S620）。他方、この検査も成功した場合には新規MT認証成功とし、認証結果1をMT9に送信する（ステップS615、S616）。この時点で無線端末MT3は無線端末MT9から送信される認証2用パケットのAPへの転送を許可する（ステップS617）。

【0210】図41のフローのステップS608で無線端末MT9が認証結果1を受信すれば、無線端末MT9～MT3間の相互認証が完了する。

【0211】このようにして無線マルチホップネットワーク中の認証済みの正規の無線端末MT3が新規の無線端末MT9を認証することで、不正無線端末が認証を裝って送信したパケットがネットワークへ流入することを防止できる。また新規無線端末は正規のProxyMTを1つ選択することで同一の認証2用パケットが複数発生し、ネットワークNWに転送されることを防止できる。

【0212】<無線端末MT～認証サーバ間の相互認証>上記の無線端末間の相互認証1の処理が成功したら、無線端末MT9は無線端末MT3、基地局AP1を介して認証サーバASと相互認証を行うことになる。

【0213】図43の新規無線端末MT側から見た認証フローの初めのステップS621で、無線端末MT9はシーケンス番号SQNを生成し、このSQNと秘密鍵SKmt9を用いてパケット検査データPCVを計算し、これらのSQN、PCVを付加した認証要求2を無線端末MT3へ送信する（ステップS622）。

【0214】図45のProxyMT側から見た認証フローのステップS661で、無線端末MT9からの認証要求2を受信した無線端末MT3は、それに添付されているPCVをシーケンス番号SQN、公開鍵PKmt9を用いて検査する（ステップS651）。もし検査が失敗した場合は、受信した認証要求2を破棄する。検査が成功した場合は、無線端末MT3はSQNと認証済み装置に配布されている無線マルチホップネットワークで共通のネットワーク鍵NK（共有鍵）を用いてパケット検査データPCVを計算する（ステップS652）。続いて無線端末MT3は、元のPCVを破棄し、新しく計算したPCVを付加した認証要求2をルート上の次装置（ここでは無線端末MT2）へ送信する（ステップS653）。

【0215】図46のフローのステップS671で、中継となる無線端末MT3は、無線端末MT9からの認証要求2を受信すれば、シーケンス番号SQNとネットワーク鍵NKを用いてパケット検査データPCVを検査し、失敗した場合は受信した認証要求2を破棄し、成功した場合はルート上の次の装置である無線端末MT2へパケットをそのまま送信する（ステップS672）。同様に、次の装置である無線端末MT2も、中継となる無線端末MT3から認証要求2を受信すれば、SQNとNKを用いてPCVを検査し、失敗した場合は受信した認

証要求2を破棄し、成功した場合はルート上の次の装置である基地局AP1へパケットをそのまま送信する（ステップS672）図45のフローのステップS651で、無線端末MT2から認証要求2を受信した基地局AP1は、パケット検査データPCVをシーケンス番号SQN、ネットワーク鍵NKを用いて検査する。もし検査が失敗した場合は、受信した認証要求2を破棄する。検査が成功した場合は、SQNと共有鍵Cap1-asを用いてPCVを計算し（ステップS652）、元のPCVを廃棄して新しいPCVを付加した認証要求2を認証サーバASへ送信する（ステップS653）。

【0216】図44に示されている認証サーバAS側から見た認証フローのステップS631で、基地局AP1から認証要求2を受信した認証サーバASは、PCVをSQN、Cap1-asを用いて検査する（ステップS632）。もし検査が失敗した場合、認証サーバASは受信した認証要求2を破棄する。検査が成功した場合、認証サーバASは続いて乱数R3を計算し、シーケンス番号SQNを生成し、そのSQN、共有鍵Cap1-asを用いてパケット検査データPCVを計算し、乱数R3とSQN、PCVを付加した認証要求応答2を基地局AP1へ送信する（ステップS633、S634）。

【0217】図45のフローのステップS651で、認証サーバASからの認証要求応答2を受信した基地局AP1は、シーケンス番号SQN、共有鍵Cap1-asを用いてパケット検査データPCVを検査する。もし検査が失敗した場合は受信した認証要求応答2を破棄する。検査が成功した場合は、基地局AP1は、シーケンス番号SQNとネットワーク鍵NKを用いて新たにパケット検査データPCVを計算し、元のPCVを破棄し、新たに計算したPCVを付加した認証要求応答2を中継となる無線端末MT2へ送信する（ステップS652、S653）。

【0218】図46のフローのステップS671で、基地局AP1からの認証要求応答2を受信した中継無線端末MT2は、SQNとNKを用いてPCVを検査し、検査が失敗した場合は受信した認証要求応答2を破棄し、検査が成功した場合はそのまま次の中継となる無線端末MT3へ送信する（ステップS672）。

【0219】ProxyMTとなっている無線端末MT3は、図45のフローのステップS651で無線端末MT2からの認証要求応答2を受信すれば、シーケンス番号SQN、ネットワーク鍵NKを用いてパケット検査データPCVを検査し、この検査が成功した場合には、SQNと秘密鍵SKmt3を用いて新たにPCVを計算し、元のPCVを破棄し、新しいPCVを付加した認証要求応答2を新規無線端末MT9へ送信する（ステップS652、S653）。

【0220】図43のフローのステップS623で、無線端末MT3からの認証要求応答2を受信した新規無線

端末MT9は、パケット検査データPCVをシーケンス番号SQN、公開鍵PKmt3を用いて検査する（ステップS624）。もし検査が失敗した場合、無線端末MT9は受信した認証要求応答2を破棄し、最初から認証2を開始する。検査が成功した場合、無線端末MT9は乱数R3、秘密鍵SKmt9を用いて署名データSigmt9を計算する（ステップS625）。無線端末MT9は続いて乱数R4を計算し、この乱数R4、自装置の証明書Certmt9、署名データSigmt9及び上記と同様の手順で計算したパケット検査データPCVを認証情報2に付加してそのパケットを無線端末MT3へ送信する（ステップS626, S627）。

【0221】図45のフローのステップS651で、認証情報2を受信したProxy無線端末MT3は、PCVを検査し、結果が正しければ新しいPCVを付加して認証情報2を次の中継とする無線端末MT2へ送信する（ステップS652, S653）。

【0222】次の中継となる無線端末MT2は、図46のフローのステップS671で無線端末MT3からの認証情報2を受信すれば、PCVを検査し、検査結果が正しければそのまま認証結果2を基地局AP1へ送信する（ステップS672）。

【0223】図45のフローのステップS651で、無線端末MT2からの認証情報2を受信した基地局AP1は、PCVを検査し、結果が正しければ新しいPCVを付加して認証結果2のパケットを認証サーバASへ送信する（ステップS652, S653）。

【0224】図44のフローのステップS635で基地局AP1からの認証情報2を受信した認証サーバASは、PCVを検査する（ステップS636）。もし検査が失敗した場合、ASは受信した認証情報2を破棄する。検査が成功した場合、ASは無線端末MT9の証明書Certmt9を検査する（ステップS637）。もし検査が失敗した場合、ASは認証失敗を示す認証結果2を新しいPCVを付加して基地局AP1へ送信する（ステップS637, S641～S643）。

【0225】無線端末MT9の証明書Certmt9の検査が成功した場合、認証サーバASはCertmt9から無線端末MT9の公開鍵PKmt9を取り出し、さらにこのPKmt9を用いてSigmt9を検査する。もし検査が失敗した場合は、認証失敗を示す認証結果2を新しいPCVを付加して基地局AP1へ送信する（ステップS637, S641～S643）。検査が成功すれば無線端末MT9は正規のMTであると判断し、認証サーバASは乱数R4、自装置の秘密鍵SKasを用いて署名データSigasを計算する（ステップS637, S638）。

【0226】次に認証サーバASは、ネットワーク鍵NKを無線端末MT9の公開鍵PKmt9で暗号化し、自装置の証明書Certasと署名データSigas、新

しいPCV、暗号化したネットワーク鍵NKを認証結果2に付加し（ステップS639）、そのパケットを基地局AP1へ送信する（ステップS640）。

【0227】認証サーバASからの認証結果2を受信すれば、基地局AP1は図45のフローのステップS651でPCVを検査する。この検査結果が正しければ新しいPCVを付加して認証結果2をMT2へ送信する（ステップS652, S653）。

【0228】図46のフローのステップS671で、中継となる無線端末MT2は基地局AP1からの認証結果2を受信すればPCVを検査し、結果が正しければそのまま認証結果2を次の無線端末MT3へ送信する（ステップS672）。

【0229】図45のフローのステップS651で、無線端末MT3は無線端末MT2からの認証結果2を受信すればPCVを検査し、結果が正しければ新しいPCVを認証結果2に付加し、そのパケットを新規の無線端末MT9へ送信する（ステップS652, S653）。

【0230】図33のフローのステップS628で、Proxy無線端末MT3からの認証結果2を受信した無線端末MT9は、PCVを検査する（ステップS629）。もし検査が失敗した場合、無線端末MT9は認証情報2を再送する。PCVの検査が成功した場合、無線端末MT9はさらに認証サーバASの証明書Certasを検査する。もし検査が失敗した場合、無線端末MT9は最初から認証2を開始する（ステップS630でNOに分岐）。検査が成功した場合、無線端末MT9は認証サーバの証明書Certasから認証サーバASの公開鍵PKasを取り出し、このPKasを用いて認証サーバの署名データSigasを検査する。もしこの検査が失敗した場合にも、無線端末MT9は最初から認証2を開始する（ステップS630でNOに分岐）。この検査が成功すれば、無線端末MT9は最終的に認証サーバASは事業者が設置した正規のASであると判断し、ネットワーク鍵NKを秘密鍵SKmt9を用いて復号化して保存し、無線端末MT9～認証サーバAS間の相互認証が完了する（ステップS630でYESに分岐）。

【0231】本発明の第9の実施の形態の無線マルチップネットワークでは、上記のように認証2用パケットにパケット検査データ(PCV)を付加することで経路上の無線端末MT、基地局APは正規のMTから送信されたパケットであることを確認するようにしたので、認証2を利用した攻撃を防止することができる。また、認証サーバASは無線端末MTから送信された認証2用パケットが正規の基地局APを経由して送信されたことを確認できる。さらに、基地局APが無線端末MTを認証した後に認証サーバASがMTを認証することで、事業者はどの基地局APにどの無線端末MTがアクセスしているかを把握できる。

【0232】[第10の実施の形態] 第9の実施の形態

では、図4 1にフローに示したMT間の認証処理の新規MT側の処理において、ステップS602の認証要求応答1の受信により、複数の無線端末及び基地局からの応答を受信した場合、ステップS603でそのすべてについて認証処理を実行し、認証が成功した無線端末が複数ある場合には、ステップS605において基地局を優先的に選択し、また基地局が含まれていない場合には複数の無線端末のうち、基地局までのホップ数が最小のものを選択するようにした。しかしながら、複数の無線端末、基地局からProxy端末を選択するロジックはこれに限らず、例えば、基地局、無線端末を区別せず、最先に応答を受信した基地局又は無線端末から順に認証処理を行い、認証が成功した無線端末又は基地局をProxy端末として選択する方法を採用することもできる。

【0233】第10の実施の形態の無線マルチホップネットワークは、この選択手順を採用したことと特徴とする。すなわち、第9の実施の形態と同様に図34～図37の機能構成を有する無線マルチホップネットワークにおいては、各無線端末MTの無線端末選択機能308が図47のMT間認証処理を実施する。

【0234】図38に示す状況において、新規の無線端末MT9がブロードキャストで認証要求1を送信し（ステップS601）、複数の無線端末や基地局から認証要求応答1が返信されてきたとする。ここでは、複数の無線端末MT3、MT4、MT8からの認証要求応答1を受信したとする（ステップS602）。

【0235】このとき無線端末MT9は、まず、最先に応答を受信した無線端末又は基地局を選択する（ここでは無線端末MT3を選択したとする。ステップS604-1）。そして、その認証要求応答1に添付された証明書Certmt3を検査する（ステップS604-2）。検査が失敗した場合は、受信した認証要求応答1を破棄し、次に応答を受信した無線端末又は基地局を選択して再度証明書の検査を実施する手順を繰り返す（ステップS604-1、S604-2、S604-3）。

【0236】ステップS604-2で証明書の検査が成功した場合は、その証明書から公開鍵PKmt3を取り出し、その公開鍵を用いて署名データSigmt3を検査する（ステップS604-2）。この検査が失敗した場合にも、受信した認証要求応答1を破棄し、次に応答を受信した無線端末又は基地局を選択して再度証明書の検査を実施する手順を繰り返す（ステップS604-1、S604-2、S604-3）。そして、両方の検査が成功した中継MTが1つもない場合には、最初に戻り、認証要求1のブロードキャストからやり直す（ステップS604-3でNOに分岐）。両方の検査が成功した中継MTがあれば、ステップS604-2でYESに分岐する。ここでも、無線端末MT3が選択されたものとする（ステップS605）。

【0237】無線端末MT9は続いて、乱数R2と自装

置の秘密鍵SKmt9を用いて署名データSigmt9を計算し、これらR2、Sigmt9、自装置の証明書Certmt9を付加した認証情報1をProxyMT（ここではMT3）へ送信する（ステップS606、S607）。

【0238】無線端末MT9により選択された無線端末MT3は、以降、第9の実施の形態と同様に図42のフローのステップS614でMT9からの認証情報1を受信すると、新規無線端末MT9の証明書Certmt9を検査する。もし検査が失敗した場合は、認証失敗を示す認証結果1をMT9へ送信する（ステップS615、S618～S620）。

【0239】検査が成功した場合は、Certmt9から公開鍵PKmt9を取り出し、この公開鍵PKmt9を用いて無線端末MT9の署名データSigmt9を検査する。もしこの検査が失敗した場合にも、無線端末MT3は認証失敗を示す認証結果1を無線端末MT9へ送信し、MT3はMT9から送信される認証2用パケットのAPへの転送を不許可にする（ステップS615、S618～S620）。他方、この検査も成功した場合には新規MT認証成功とし、認証結果1をMT9に送信する（ステップS615、S616）。この時点で無線端末MT3は無線端末MT9から送信される認証2用パケットのAPへの転送を許可する（ステップS617）。

【0240】図41のフローのステップS608で無線端末MT9が認証結果1を受信すれば、無線端末MT9～MT3間の相互認証が完了する。

【0241】このようにして無線マルチホップネットワーク中の認証済みの正規の無線端末MT3が新規の無線端末MT9を認証することで、不正無線端末が認証を裝って送信したパケットがネットワークへ流入することを防止できる。また新規無線端末は正規のProxyMTあるいは基地局を1つ選択することで同一の認証2用パケットが複数発生し、ネットワークNWに転送されることを防止できる。加えて、第10の実施の形態の場合、最先に応答のあった無線端末又は基地局から優先的にプロキシ端末として選択することで、実質的な通信処理速度を速めることができる。

【0242】【第11の実施の形態】本発明の第11の実施の形態の無線マルチホップネットワークについて、図48を用いて説明する。第11の実施の形態の無線マルチホップネットワークは、第9の実施の形態と同様に図34～図37の機能構成を有する無線マルチホップネットワークにおいては、各無線端末MTの無線端末選択機能308が図48のMT間認証処理を実施することを特徴とする。

【0243】すなわち、新規の無線端末MTがMT間の認証処理において、複数の無線端末、基地局から認証要求応答1を受信した場合に、受信レベルの高い基地局又は無線端末から順に認証処理を行い、認証が成功した無

線端末又は基地局をProxy端末として選択するようにしたことを特徴とする。

【0244】図38に示す状況において、新規の無線端末MT9がブロードキャストで認証要求1を送信し（ステップS601）、複数の無線端末や基地局から認証要求応答1が返信されてきたとする。ここでは、複数の無線端末MT3, MT4, MT8からの認証要求応答1を受信したとする（ステップS602）。

【0245】このとき無線端末MT9は、まず、応答信号の受信レベルの最も高い無線端末又は基地局を選択する（ここでも無線端末MT3を選択したとする。ステップS604-11）。そして、その認証要求応答1に添付された証明書Certmt3を検査する（ステップS604-2）。検査が失敗した場合は、受信した認証要求応答1を破棄し、次に応答を受信した無線端末又は基地局を選択して再度証明書の検査を実施する手順を繰り返す（ステップS604-11, S604-2, S604-3）。

【0246】ステップS604-2で証明書の検査が成功した場合は、その証明書から公開鍵PKmt3を取り出し、その公開鍵を用いて署名データSigmt3を検査する。この検査が失敗した場合にも、受信した認証要求応答1を破棄し、次に応答を受信した無線端末又は基地局を選択して再度証明書の検査を実施する手順を繰り返す（ステップS604-11, S604-2, S604-3）。そして、両方の検査が成功した中継MTが1つもない場合には、最初に戻り、認証要求1のブロードキャストからやり直す（ステップS604-3でNOに分岐）。

【0247】両方の検査が成功した中継MTがあれば、ステップS604-2でYESに分岐する。ここでも、無線端末MT3が選択されたものとする（ステップS605）。以降の処理は第10の実施の形態と共通である。

【0248】このようにして無線マルチホップネットワーク中の認証済みの正規の無線端末MT3が新規の無線端末MT9を認証することで、不正無線端末が認証を裝って送信したパケットがネットワークへ流入することを防止できる。また新規無線端末は正規のProxyMTあるいは基地局を1つ選択することで同一の認証2用パケットが複数発生し、ネットワークNWに転送されることを防止できる。加えて、第11の実施の形態の場合、応答信号の受信レベルが高い無線端末又は基地局から優先的にプロキシ端末として選択することで、通信の信頼性を高めることができる。

【0249】[第12の実施の形態] 本発明の第12の実施の形態の無線マルチホップネットワークについて、図49を用いて説明する。第12の実施の形態の無線マルチホップネットワークは、第9の実施の形態と同様に図34～図37の機能構成を有する無線マルチホップネ

ットワークにおいては、各無線端末MTの無線端末選択機能308が図49のMT間認証処理を実施することを特徴とする。

【0250】すなわち、新規の無線端末MTがMT間の認証処理において、複数の無線端末、基地局から認証要求応答1を受信した場合に、基地局APまでのホップ数が最も少ない無線端末から順に認証処理を行い、認証が成功した無線端末又は基地局をProxy端末として選択するようにしたことを特徴とする。

【0251】図38に示す状況において、新規の無線端末MT9がブロードキャストで認証要求1を送信し（図49のステップS601）、複数の無線端末や基地局から認証要求応答1が返信されてきたとする。ここでは、複数の無線端末MT3, MT4, MT8からの認証要求応答1を受信したとする（ステップS602）。

【0252】このとき無線端末MT9は、基地局までのホップ数が最も少ない無線端末を選択し、又は基地局からの認証要求応答1を直接に受信したのであればその基地局をそのまま選択する（ここでも無線端末MT3を選択したとする。ステップS604-21）。そして、その認証要求応答1に添付された証明書Certmt3を検査する（ステップS604-2）。検査が失敗した場合は、受信した認証要求応答1を破棄し、基地局までのホップ数がその次に少ない無線端末を選択して再度証明書の検査を実施する手順を繰り返す（ステップS604-11, S604-2, S604-3）。

【0253】ステップS604-2で証明書の検査が成功した場合は、その証明書から公開鍵PKmt3を取り出し、その公開鍵を用いて署名データSigmt3を検査する。この検査が失敗した場合にも、受信した認証要求応答1を破棄し、基地局までのホップ数がその次に少ない無線端末を選択して再度証明書の検査を実施する手順を繰り返す（ステップS604-21, S604-2, S604-3）。そして、両方の検査が成功した中継MTが1つもない場合には、最初に戻り、認証要求1のブロードキャストからやり直す（ステップS604-3でNOに分岐）。

【0254】両方の検査が成功した中継MTがあれば、ステップS604-2でYESに分岐する。ここでも、無線端末MT3が選択されたものとする（ステップS605）。以降の処理は第10の実施の形態と共通である。

【0255】このようにして無線マルチホップネットワーク中の認証済みの正規の無線端末MT3が新規の無線端末MT9を認証することで、不正無線端末が認証を裝って送信したパケットがネットワークへ流入することを防止できる。また新規無線端末は正規のProxyMTあるいは基地局を1つ選択することで同一の認証2用パケットが複数発生し、ネットワークNWに転送されることを防止できる。加えて、第12の実施の形態の場合、

基地局までのホップ数が少ない無線端末から優先的にプロキシ端末として選択することで、通信の信頼性と応答速度を高めることができる。

【0256】なお、本発明は上記のすべての実施の形態において無線端末、基地局、認証サーバそれぞれが果たす図示フローチャート各々の諸機能を実現させるために各装置に組み込んで実行させるソフトウェアプログラムも権利対象とするものである。

【0257】

【発明の効果】請求項1の発明の無線アクセสนetworkによれば、認証サーバ(AS)と基地局(AP)が相互認証を行うことで、事業者が一般ユーザの設置したAPの安全性を保障することができる。また、新規無線端末(MT)がアクセスしたとき、最初にMT-AP間で相互認証することで互いが正当な装置であるか否かを確認することができ、APはこの相互認証が成功するまでは新規MTが送信したパケットを事業者側ネットワークに転送しないので、認証を装ったDoS攻撃を防止することができる。さらに、MT-AP間の相互認証成功後にMT-AS間の相互認証及びこの認証用パケットのパケット検査(送信元確認)を行うことで、ASはどのAPにどのMTがアクセスしたかを正確に把握して管理することができる。

【0258】請求項2の発明の無線マルチホップネットワークによれば、新規無線端末(MT)が無線マルチホップネットワークにアクセスしたとき、最初に新規MT-近隣MT間で相互認証することで互いが正当な装置であるか否かを確認することができ、近隣のMTはこの相互認証が成功するまでは新規MTが送信したパケットを無線マルチホップネットワークに転送しないので、認証を装ったDoS攻撃を防止することができる。また、相互認証の際にMT-AS(認証サーバ)間相互認証用パケットを中継させるMT又はAP(基地局)を1つ選択することで、同じ認証処理が同時に複数発生してしまうことを防止する。さらに、MT-AP間の相互認証成功後にMT-AS間の相互認証及びこの認証用パケットのパケット検査(送信元確認)を行うことでASはどのAPにどのMTがアクセスしたかを正確に把握して管理することができる。

【0259】請求項3の発明の無線端末(MT)によれば、無線アクセสนetworkに新規に参入するときに基地局(AP)と相互認証を行い、その成功の後に認証サーバ(AS)と相互認証を行う機能を備えたことで、APに新規MTとの相互認証が成功するまで新規MTの送信したパケットを事業者側ネットワークに転送しない機能を持たせることによって、当該MTを用いなければAPとの通信、ひいては認証サーバ(AS)との通信ができない無線アクセสนetworkを構築することができ、認証を装ったDoS攻撃に耐性の強い無線アクセสนetworkの構築に寄与できる。

【0260】請求項4の発明の無線端末によれば、送信する認証用パケットに送信元を示すパケット検査データを算出して添付する機能を備えたので、認証用パケットにパケット検査データを添付することにより、受信先の基地局に送信元を明かすことができ、不正な攻撃のために用いられなくなる。

【0261】請求項5~8の発明の無線端末(MT)によれば、新規MTはMT-AP(基地局)間相互認証の際にMT-AS(認証サーバ)間相互認証用パケットを中継させるAP又はMTを所定のロジックにしたがって選択することで、同じ認証処理が同時に複数発生してしまうことを防止することができる。

【0262】請求項9の発明の認証サーバ(AS)によれば、基地局(AP)と相互認証を行い、また新規無線端末(MT)とも相互認証を行い、しかも新規無線端末との相互認証の際には認証用パケットに添付されている送信元を示すパケット検査データを検査し、この検査が成功すれば相互認証を実施することになるので、不正なAPを排除し、正規のAPだけを管理することができ、またどのAPにどのMTがアクセスしたかをも正確に把握することができる。

【0263】請求項10の発明の認証サーバ(AS)によれば、自身の認証した無線端末(MT)の移動を管理し、MTがある基地局(AP)から別のAPへ移動した時、MT-AS間の相互認証が成功した後に、そのMTが属していた旧APへ当該MTが移動したことを通知することにより、APに一度は相互認証したがいまでは移動して通信できなくなったMTの記録をいつまでも保持させなくともよく、APにおけるMTの管理データを少なくでき、それだけ処理の高速化が図れる。

【0264】請求項11の発明の基地局(AP)によれば、新規に無線アクセสนetwork又は無線マルチホップネットワークに接続するときには必ず認証サーバと相互認証を実施するため、不正にAPを設置することを困難にし、事業者が一般ユーザの設置したAPの安全性を保障することができる。

【0265】請求項12の発明の基地局(AP)によれば、新規無線端末(MT)がアクセスしてきたとき、最初にMT-AP間で相互認証することでMTが正当な装置であるか否かを確認し、この相互認証が成功するまでは新規MTが送信したパケットを事業者側ネットワークに転送しないので、認証を装ったDoS攻撃を防止することができる。

【0266】請求項13の発明の基地局によれば、相互認証に成功した無線端末それぞれの情報を自装置に登録する機能と、認証サーバから移動通知を受けて、該当する無線端末の登録情報を削除する機能とを備えたので、無線端末が他の基地局の通信エリアに移動した場合に、通信ができなくなってしまった無線端末の情報を削除することによって無線端末の管理のためのリソースを節約

できる。

【0267】請求項14の発明の無線端末(MT)によれば、無線マルチホップネットワークに新規にアクセスするとき、最初に近隣MT又はAPとの間で相互認証する機能を備えたことで、当該MTが新規に無線マルチホップネットワークに参入する際には近隣のMT又はAPに正当な装置であるか否かを確認させ、近隣のMT又はAPはこの相互認証が成功するまでは当該MTが送信したパケットを無線マルチホップネットワークに転送しないので、認証を装ったDOS攻撃に対する耐性の高い無線マルチホップネットワークの構築に寄与できる。また、相互認証の際にMT-AS(認証サーバ)間相互認証用パケットを中継させるMT又はAP(基地局)を1つ選択する機能を備えたことで、同じ認証処理が同時に複数発生してしまうことを防止することができる。

【0268】請求項15の発明の無線端末(MT)によれば、自装置が新規に無線マルチホップネットワークにアクセスするときに、無線端末間認証用パケットを近隣の無線端末又は基地局に送信する機能と、自装置が新規無線端末である場合に、無線端末-認証サーバ間認証用パケットに送信元を示すパケット検査データを添付して送信する機能と、自装置が他の新規無線端末によって選択されたプロキシ端末である場合には、他の新規無線端末から送信された無線端末-認証サーバ間認証用パケットに対してパケット検査データを検査し、検査が失敗すればその認証用パケットを破棄し、当該検査が成功すれば当該認証用パケットに自装置で算出した送信元を示すパケット検査データを添付してルート上の他の無線端末又は基地局に対して転送する機能とを備えたので、どの基地局(AP)にどの無線端末(MT)がアクセスしたかを認証サーバに正確に把握させることができる。

【0269】請求項16～18の発明の無線端末(MT)によれば、MT-AP(基地局)間相互認証の際にMT-AS(認証サーバ)間相互認証用パケットを中継させるAP又はMTとして最適なものを選択する機能を備えたことで、同じ認証処理が同時に複数発生してしまうことを防止することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態の無線アクセスマルチホップネットワークの機能構成のブロック図。

【図2】第1の実施の形態における認証サーバの機能ブロック図。

【図3】第1の実施の形態における基地局の機能ブロック図。

【図4】第1の実施の形態における無線端末の機能ブロック図。

【図5】第1の実施の形態における基地局(AP)-認証サーバ(AS)間の認証シーケンス図。

【図6】第1の実施の形態におけるAP-AS間の認証用パケットのペイロードデータの説明図。

【図7】第1の実施の形態において実施するAP-AS間認証におけるAP側の認証処理のフローチャート。

【図8】第1の実施の形態において実施するAP-AS間認証におけるAS側の認証処理のフローチャート。

【図9】第1の実施の形態における無線端末(MT)-認証サーバ(AS)間の認証シーケンス図。

【図10】第1の実施の形態におけるMT-AS間の認証用パケットのペイロードデータの説明図。

【図11】第1の実施の形態において実施するMT-AP間認証におけるMT側の認証処理のフローチャート。

【図12】第1の実施の形態において実施するMT-AP間認証におけるAP側の認証処理のフローチャート。

【図13】第1の実施の形態において実施するMT-AS間認証におけるMT側の認証処理のフローチャート。

【図14】第1の実施の形態において実施するMT-AS間認証におけるAS側の認証処理のフローチャート。

【図15】第1の実施の形態において実施するMT-AS間認証におけるAP側の認証結果2以外のパケット受信時の認証処理のフローチャート。

【図16】第1の実施の形態において実施するMT-AS間認証におけるAP側の認証結果2のパケット受信時の認証処理のフローチャート。

【図17】本発明の第2の実施の形態の無線アクセスマルチホップネットワークにおける基地局密度が高い環境での1つの無線端末(MT)が複数の基地局(AP)と通信する状況を示す説明図。

【図18】第2の実施の形態における無線端末の機能構成のブロック図。

【図19】第2の実施の形態における無線端末の機能ブロック図。

【図20】第2の実施の形態において実施するMT-認証サーバ(AS)間の認証シーケンス図。

【図21】第2の実施の形態におけるMTのAP選択処理のフローチャート。

【図22】本発明の第3の実施の形態の無線アクセスマルチホップネットワークにおけるMTのAP選択処理のフローチャート。

【図23】本発明の第4の実施の形態の無線アクセスマルチホップネットワークにおけるMTのAP選択処理のフローチャート。

【図24】本発明の第5の実施の形態の無線アクセスマルチホップネットワークにおけるMTのAP選択処理のフローチャート。

【図25】本発明の第6の実施の形態の無線アクセスマルチホップネットワークにおけるMTのAP選択処理のフローチャート。

【図26】本発明の第7の実施の形態の無線アクセスマルチホップネットワークにおけるMTのAP選択処理のフローチャート。

【図27】本発明の第8の実施の形態の無線アクセスマルチホップネットワークにおけるMTのAP選択処理のフローチャート。

ットワークにおける認証サーバ（AS）の機能構成のブロック図。

【図28】第8の実施の形態における基地局（AP）の機能構成のブロック図。

【図29】第8の実施の形態における認証サーバ（AS）の機能ブロック図。

【図30】第8の実施の形態における基地局（AP）の機能ブロック図。

【図31】第8の実施の形態によるASのAPに対するリソース開放処理のシーケンス図。

【図32】上記のリソース開放処理に用いるパケットフォーマットの説明図。

【図33】第8の実施の形態におけるASのMT移動管理処理のフローチャート。

【図34】本発明の第9の実施の形態の無線マルチホップネットワークの機能構成のブロック図。

【図35】第9の実施の形態における認証サーバの機能ブロック図。

【図36】第9の実施の形態における基地局の機能ブロック図。

【図37】第9の実施の形態における無線端末の機能ブロック図。

【図38】第9の実施の形態の無線アクセสนットワークの動作説明図。

【図39】第9の実施の形態において実施する無線端末（MT）—認証サーバ（AS）間の認証シーケンス図。

【図40】第9の実施の形態において使用するMT—AS間の認証用パケットのペイロードデータの説明図。

【図41】第9の実施の形態において実施するMT—MT間認証における新規MT側の認証処理のフローチャート。

【図42】第9の実施の形態において実施するMT—MT間認証におけるProxy MT側の認証処理のフローチャート。

【図43】第9の実施の形態において実施するMT—AS間認証における新規MT側の認証処理のフローチャート。

【図44】第9の実施の形態において実施するMT—AS間認証におけるAS側の認証処理のフローチャート。

【図45】第9の実施の形態において実施するMT—AS間認証におけるProxy MT側又は基地局（AP）側の認証2用パケット受信時の認証処理のフローチャート。

【図46】第9の実施の形態において実施するMT—AS間認証における中継MT側のパケット中継処理のフローチャート。

【図47】本発明の第10の実施の形態の無線マルチホップネットワークにおいて実施するMT間認証における新規MT側の認証処理のフローチャート。

【図48】本発明の第11の実施の形態の無線マルチホップネットワークにおいて実施するMT間認証における新規MT側の認証処理のフローチャート。

【図49】本発明の第12の実施の形態の無線マルチホップネットワークにおいて実施するMT間認証における新規MT側の認証処理のフローチャート。

【図50】従来から提案されている無線アクセสนットワークの機能構成のブロック図。

【図51】従来から提案されている無線アクセสนットワークに対するDoS攻撃の説明図。

【図52】従来から提案されている無線アクセสนットワークにおける認証処理の多重発生のメカニズムの説明図。

【図53】従来から提案されている無線マルチホップネットワークの機能構成のブロック図。

【図54】従来から提案されている無線マルチホップネットワークにおける認証処理の多重発生のメカニズムの説明図。

【符号の説明】

101 無線端末との相互認証機能

102 無線端末管理機能

103 有線区間パケット検査機能

104 パケット判別機能

105 基地局との相互認証機能

106 基地局管理機能

107 無線端末移動管理機能

201 認証用パケット転送機能

202 無線区間パケット検査機能

203 有線区間パケット検査機能

204 パケット判別機能

205 パケット中継機能

206 認証サーバとの相互認証機能

207 無線端末との相互認証機能

208 パケット転送判断機能

209 無線端末管理機能

210 リソース開放機能

301 認証サーバとの相互認証機能

302 無線区間パケット検査機能

303 パケット判別機能

304 パケット中継機能

305 基地局との相互認証機能

307 無線端末との相互認証機能

308 無線端末選択機能

309 パケット転送機能

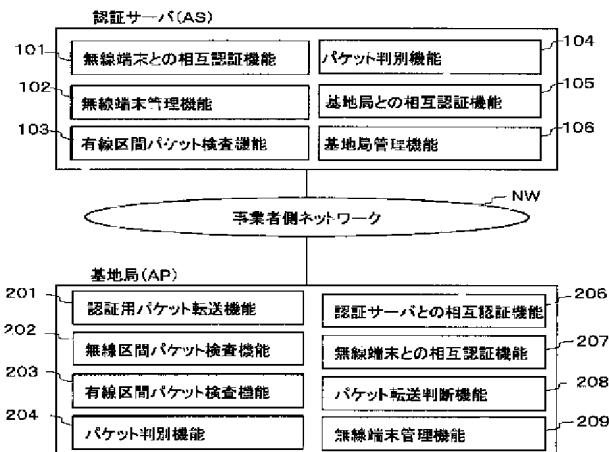
AS 認証サーバ (Authentication Server)

AP 基地局 (Access Point)

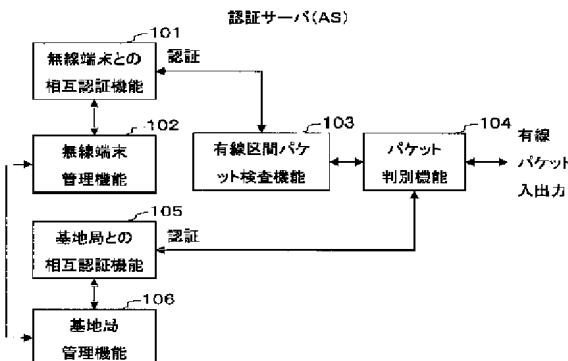
MT 無線端末 (Mobile Terminal)

NW (有線) 事業者用ネットワーク

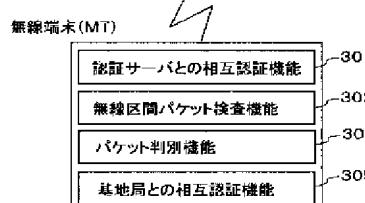
【図1】



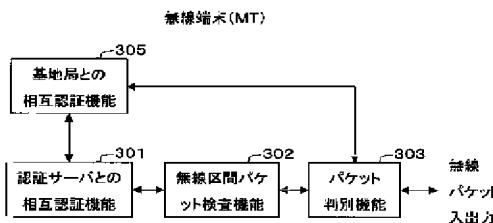
【図2】



【図4】

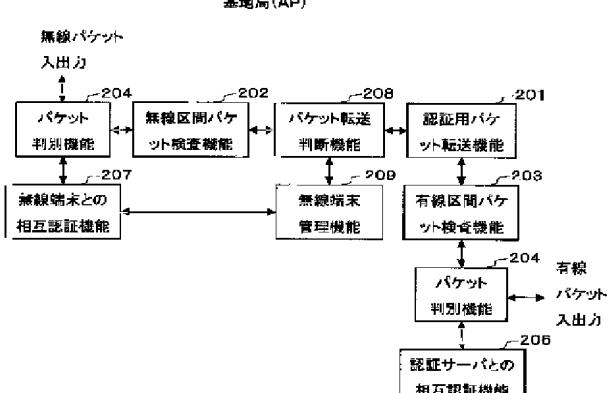


【図3】

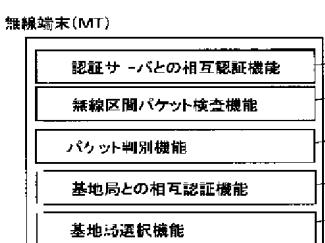


【図18】

【図32】



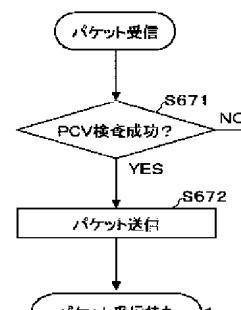
【図5】



- リソース開放通知 AS, AP1, MT
- リソース開放完了 AP1, AS, MT, Info

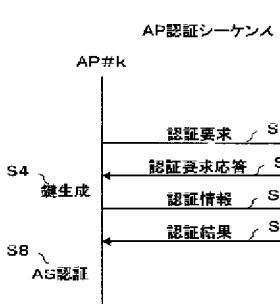
【図46】

MT-AS間認証フロー(中継MT)

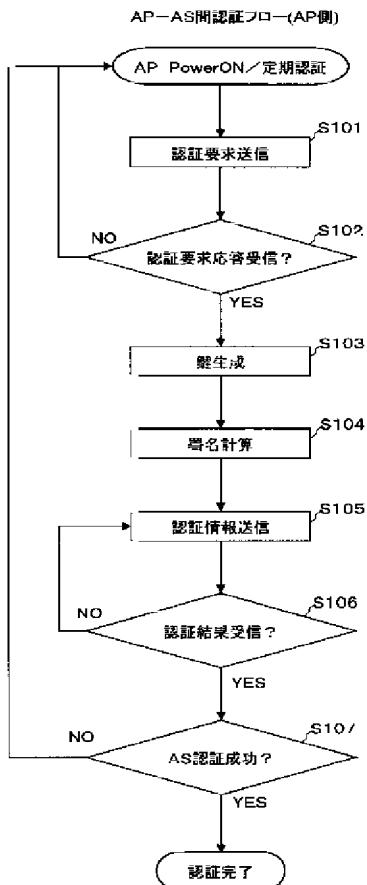


【図6】

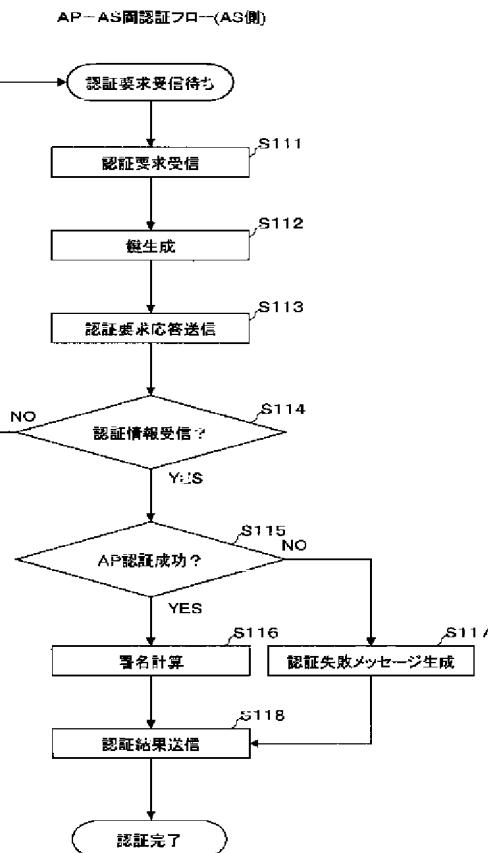
- AP認証シーケンス**
- APがk 認証要求 / S1 → AS
 - AS 認証要求応答 / S3 → APがk
 - AS 認証情報 / S5 → APがk
 - AS 認証結果 / S7 → APがk
- パケットペイロードデータ**
- 認証要求応答
 - AS, KE as, R1
 - 認証情報
 - AP#k, R2, Cert#k, Sig#k
 - Sig#k=EP(SK#k, H(AP#k, AS, R1, KE ap#k, KE as))
 - 認証結果
 - AP#k, Cert ap#k, Sig ap#k
 - Sig as=EP(SK as, H(AS, AP#k, R2, KE as, KE ap#k))
 - 認証要求
 - AP#k, KE ap#k



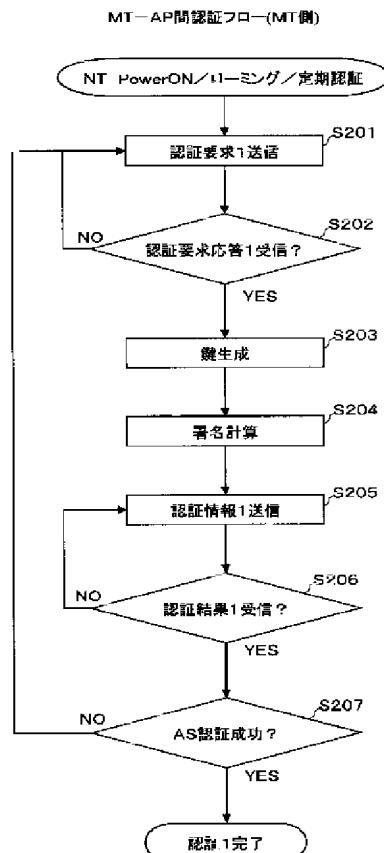
【図7】



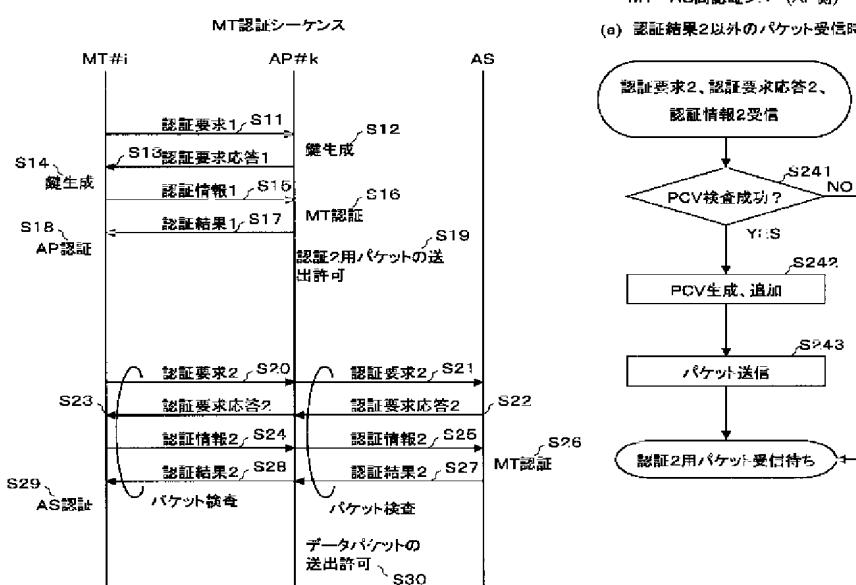
【図8】



【図11】



【図9】



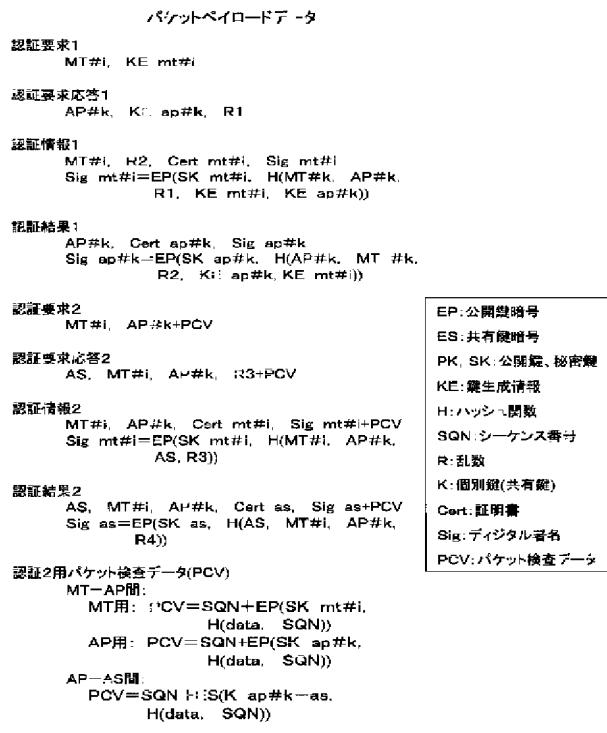
【図15】

【図27】

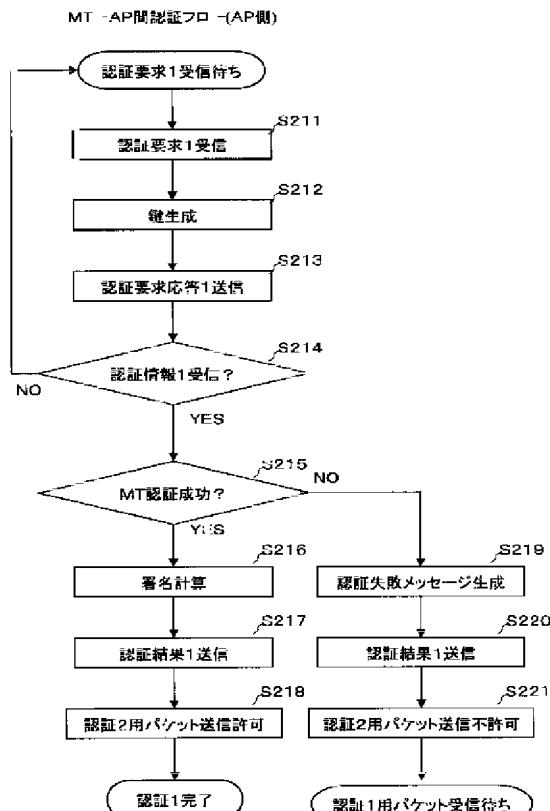
認証サーバ(AS)

無線端末との相互認証機能	101
無線端末管理機能	102
有線区間パケット検査機能	103
パケット判別機能	104
基地局との相互認証機能	105
基地局管理機能	106
無線端末移動管理機能	107

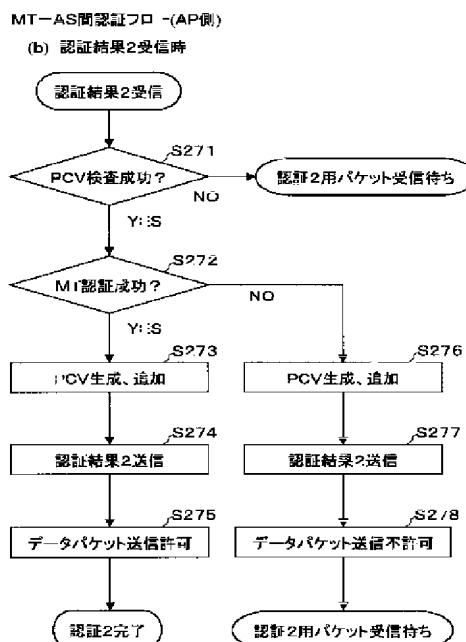
【図10】



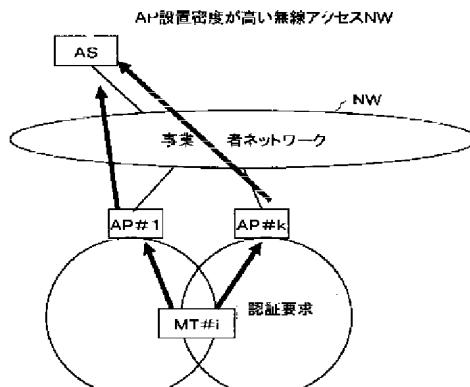
【図12】



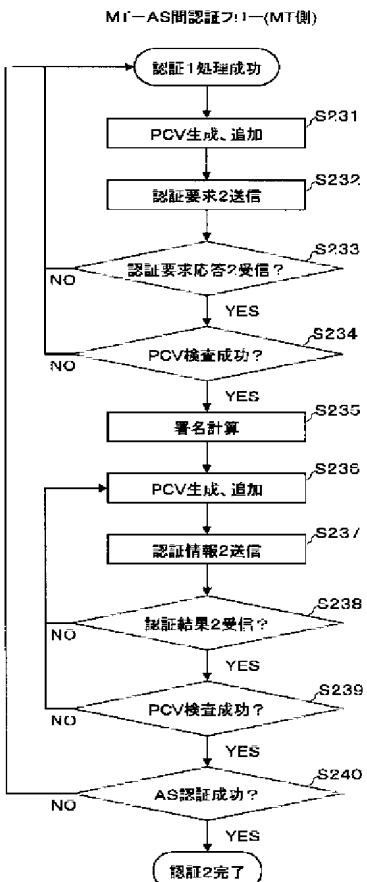
【図16】



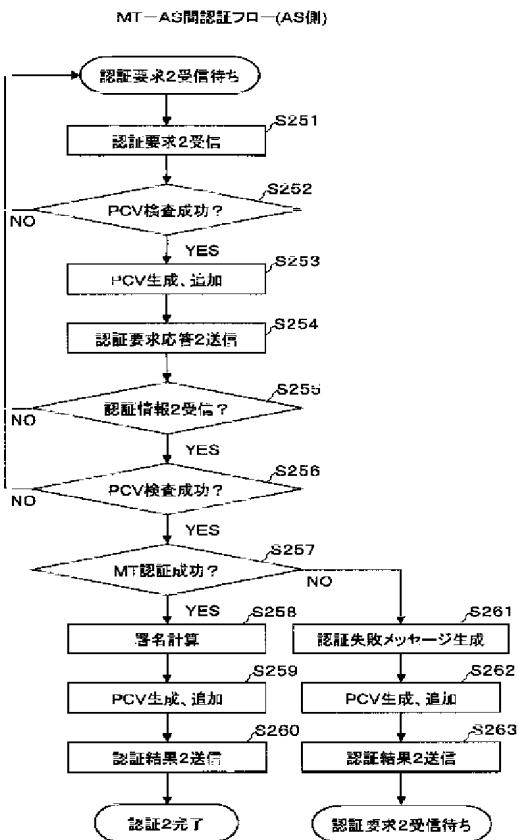
【図17】



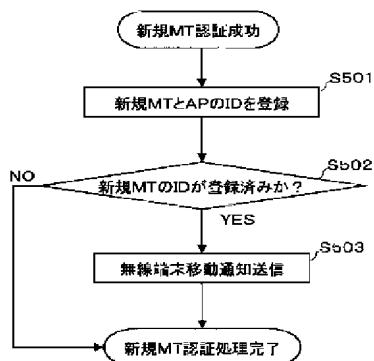
【図13】



【図14】

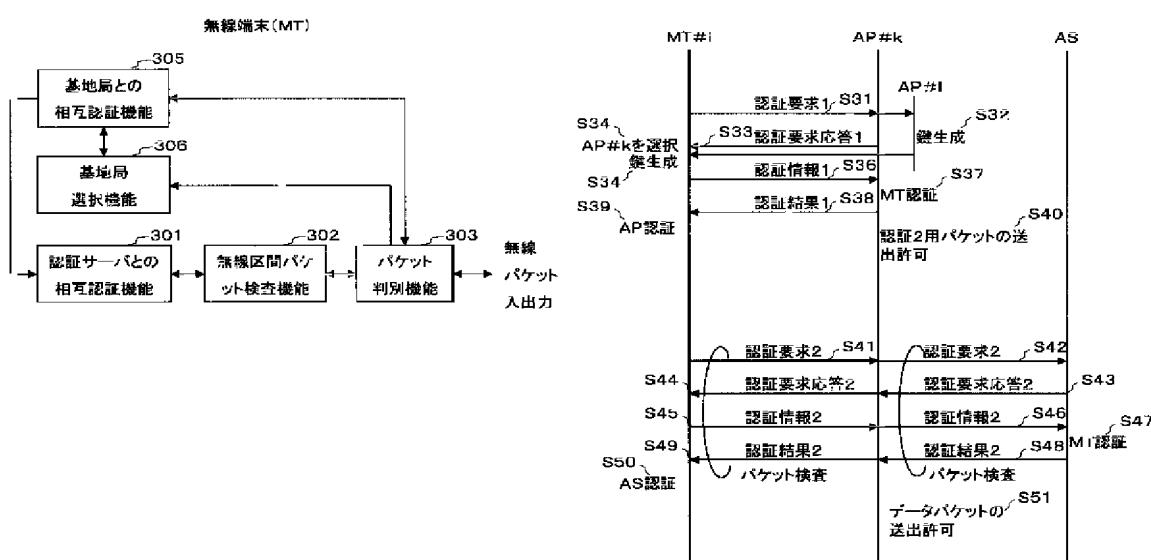


【図33】

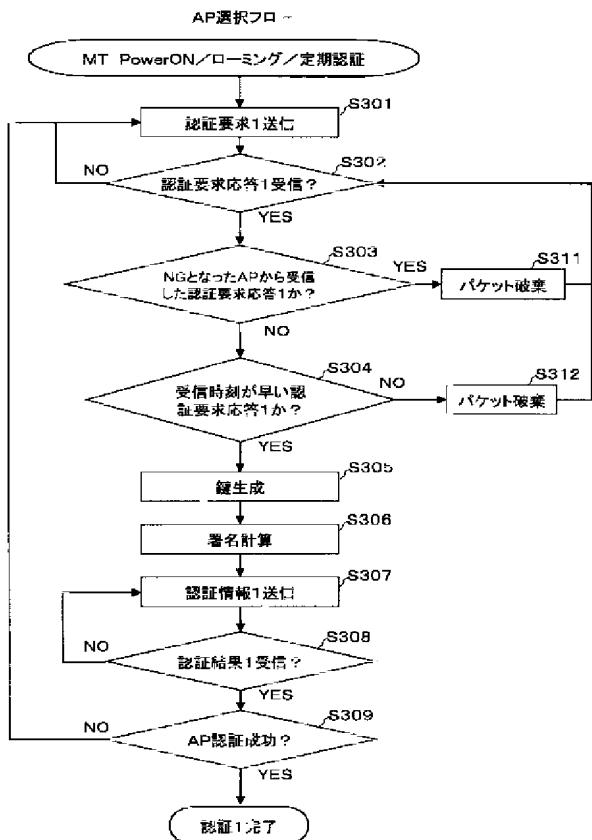


【図19】

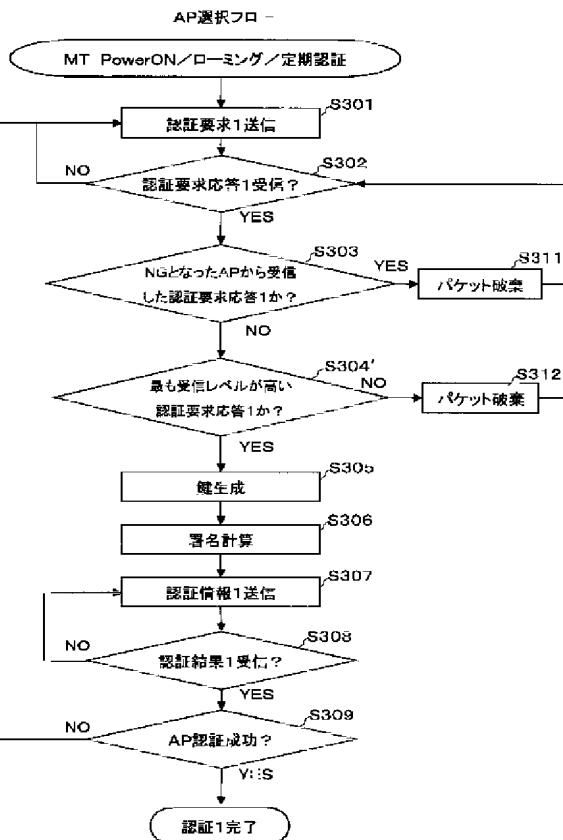
【図20】



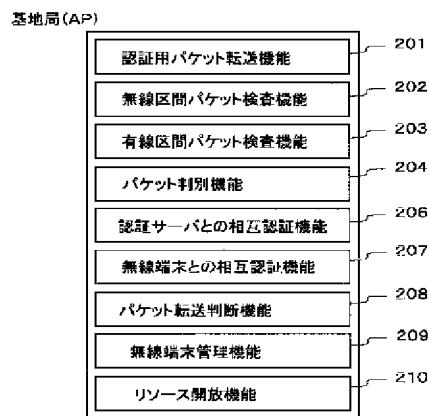
【図21】



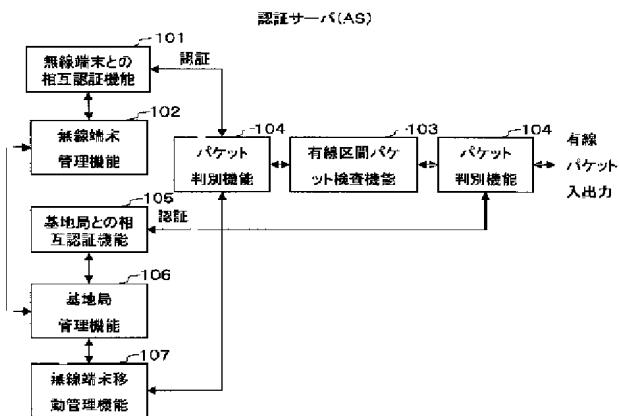
【図22】



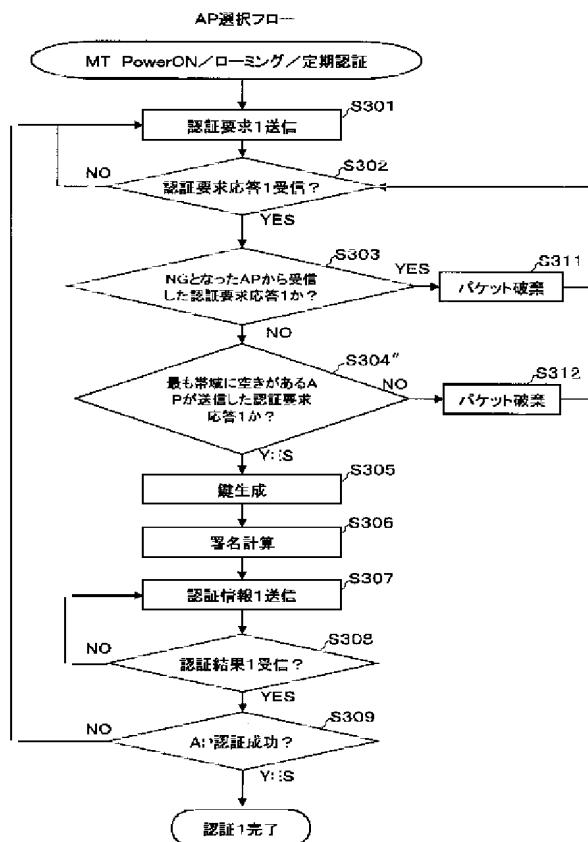
【図28】



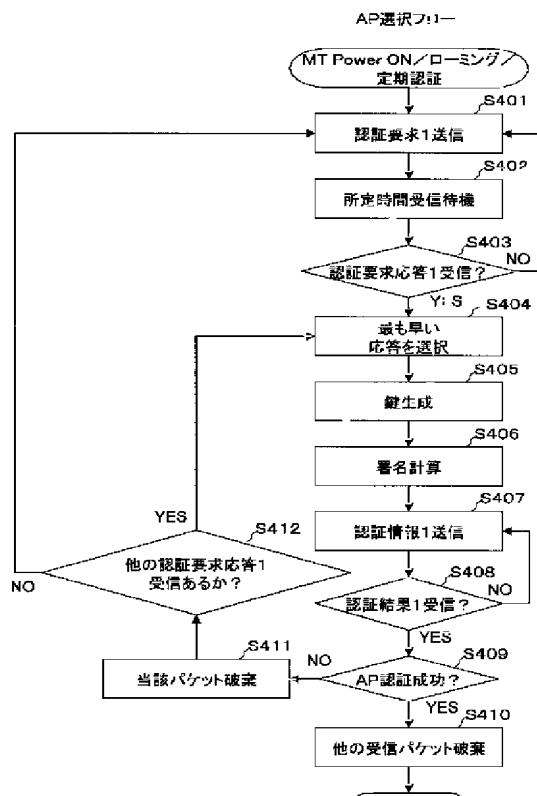
【図29】



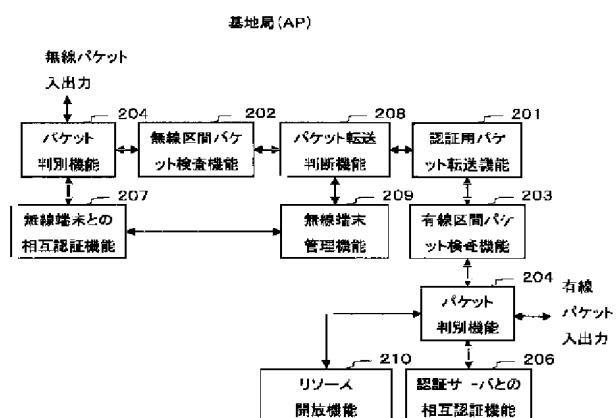
【図23】



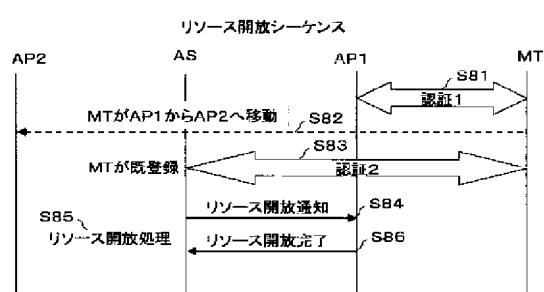
【図24】



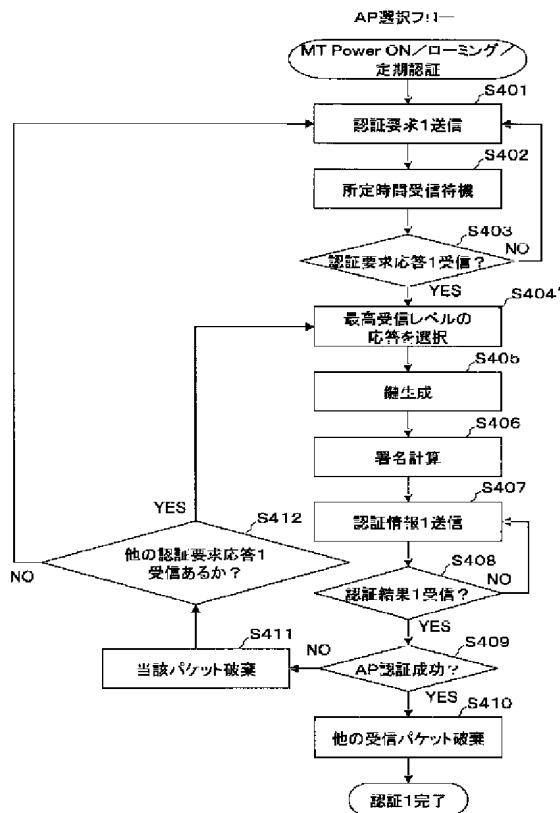
【図30】



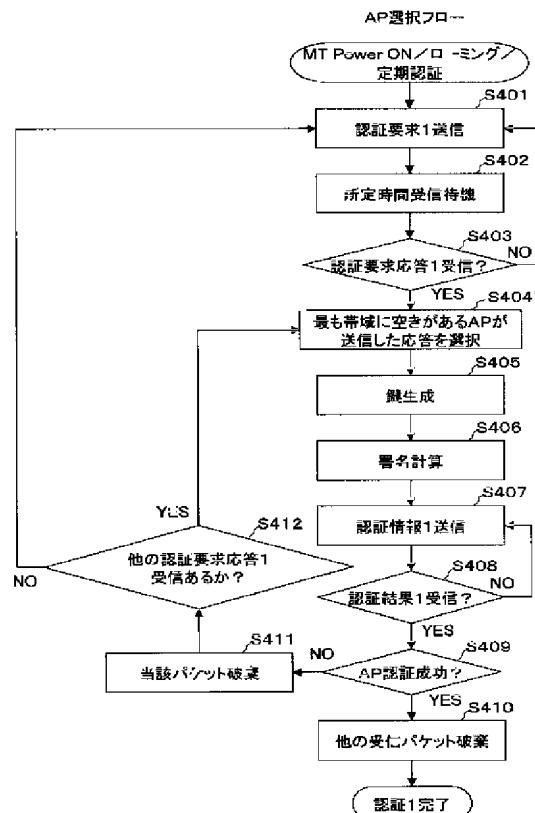
【図31】



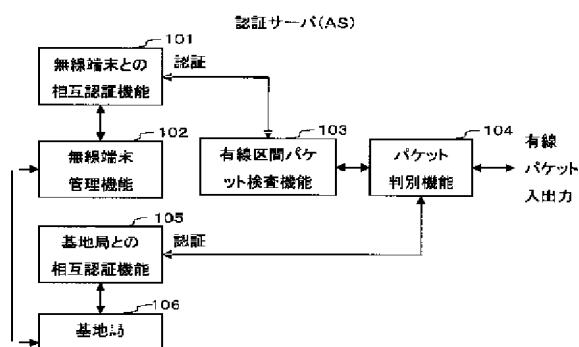
【図25】



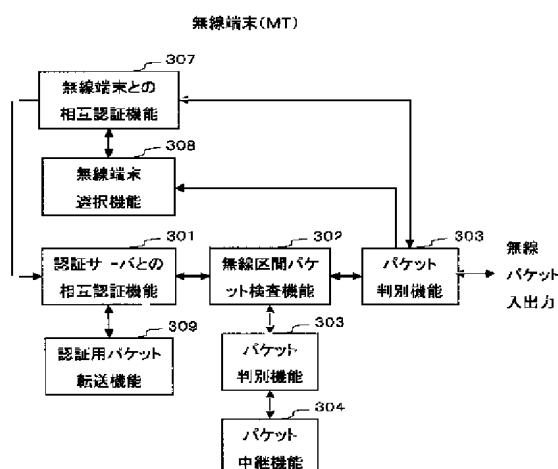
【図26】



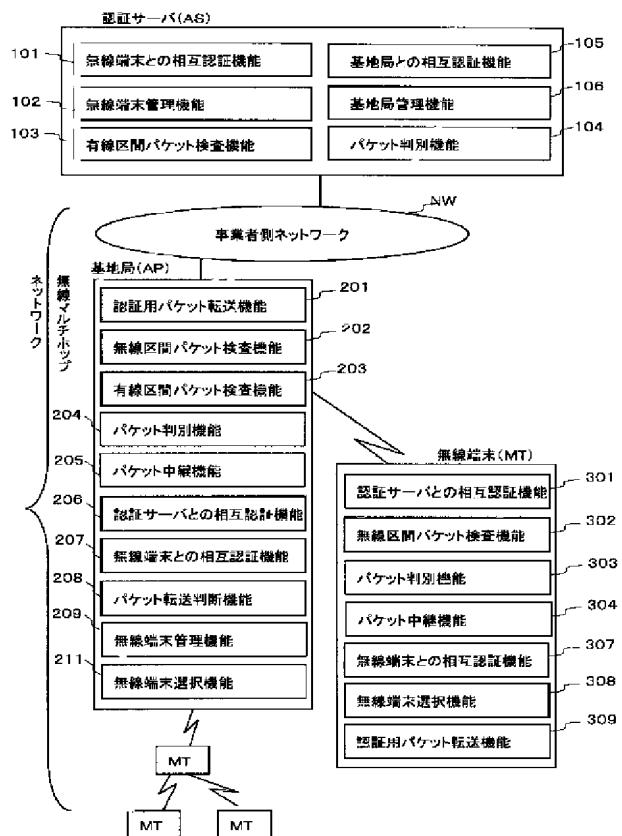
【図35】



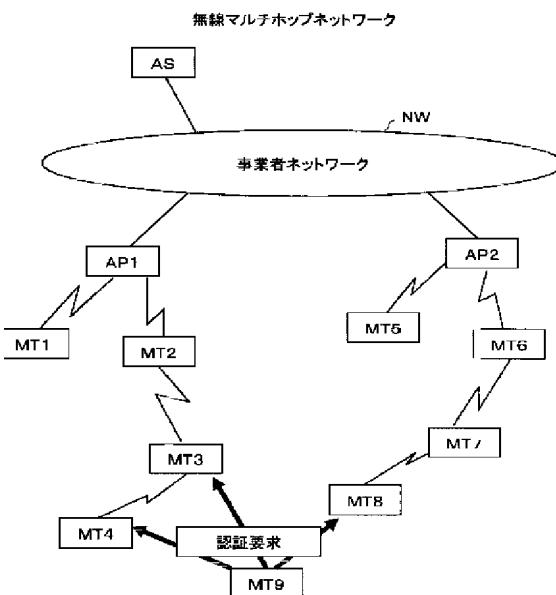
【図37】



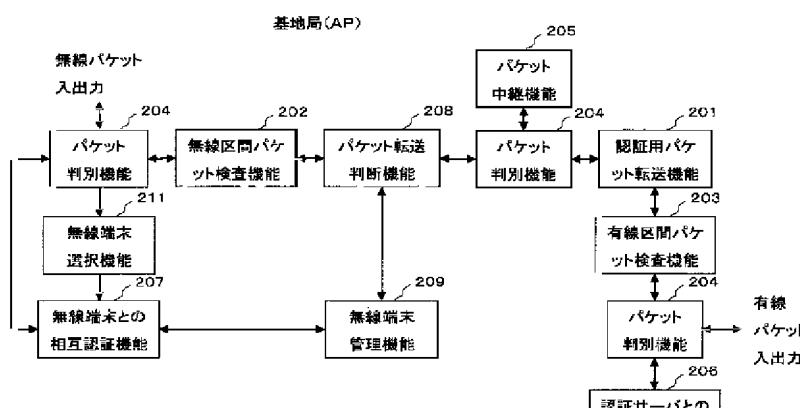
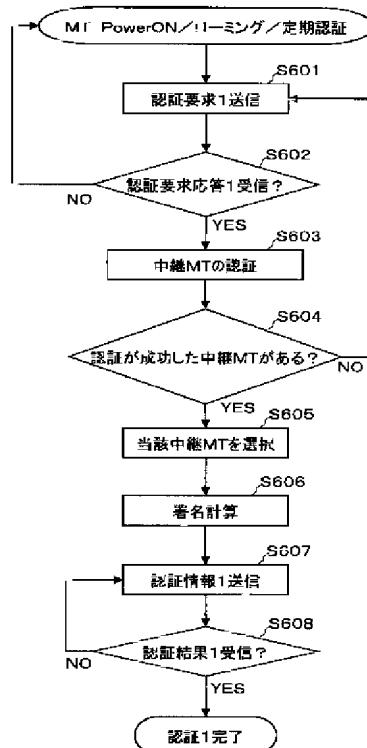
【図34】



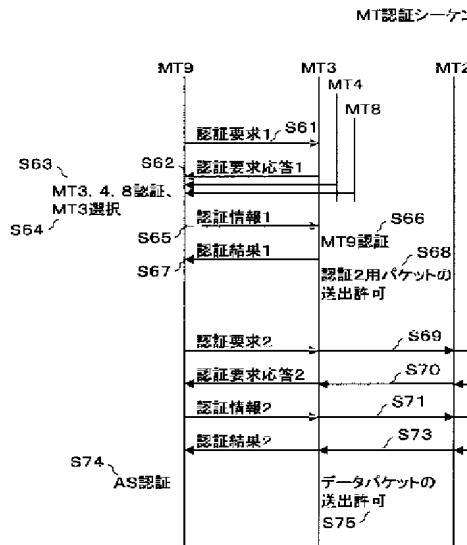
【図38】



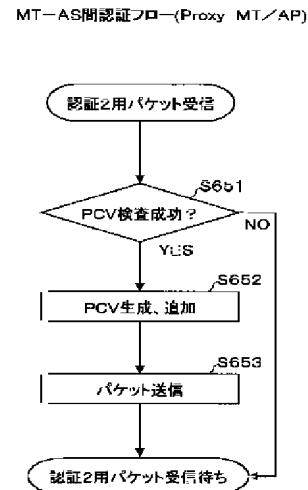
【図36】

【図41】
MT間認証フロー(新規MT側)

【図39】



【図45】



【図40】

パケットペイロードデータ

認証要求1
MT9, R1

認証要求応答1
MT3, R2, Cert mt3, Sig mt3, Rlinfo
Sig mt3=EP(SK mt3, H(MT3, MT9, R1, Rl fo))

認証情報1
MT9, Cert mt9, Sig mt9
Sig mt9=EP(SK mt9, H(MT9, MT3, R2))

認証結果1
MT3, MT9

認証要求2
MT3, AP1+PCV

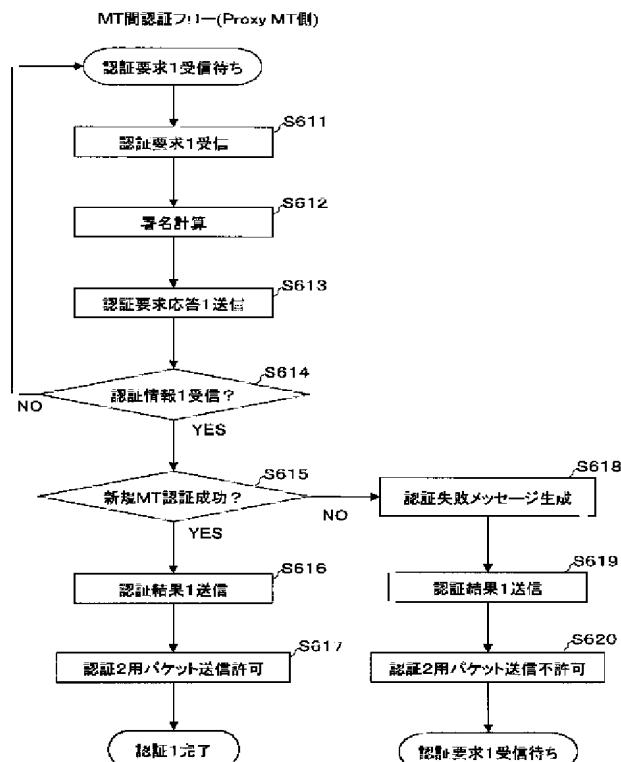
認証要求応答2
AS, MT9, AP1, R3+PCV

認証情報2
MT9, AP1, R4, Cert mt9, Sig mt9+PCV
Sig mt9=EP(SK mt9, H(MT9, AP1, AS, R3))

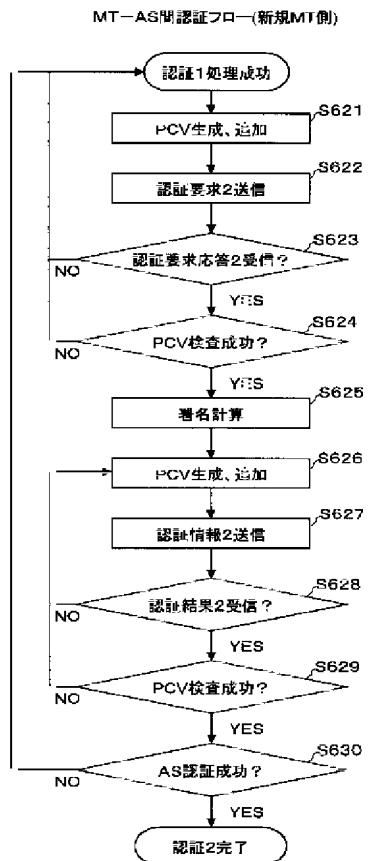
認証結果2
AS, MT9, AP1, Cert as, Sig as, [NK]+PCV
Sig as=EP(SK as, H(AS, MT9, AP1, R4))
[NK]=EP(PK mt9, NK)

認証2用パケット検査データ(PCV)
MT9-MT3間:
MT用: PCV=SQN+H(SK mt9, H(data, SQN))
AP用: PCV=SQN+EP(SK mt3, H(data, SQN))
MT3-AP1間:
PCV=SQN+ES(NK, H(data, SQN))
AP1-AS間:
PCV=SQN+ES(K as-as, H(data, SQN))

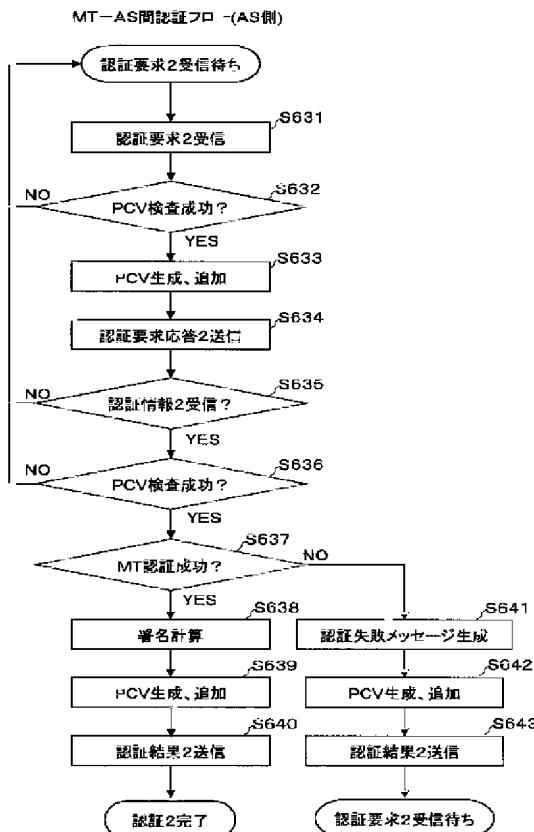
【図42】



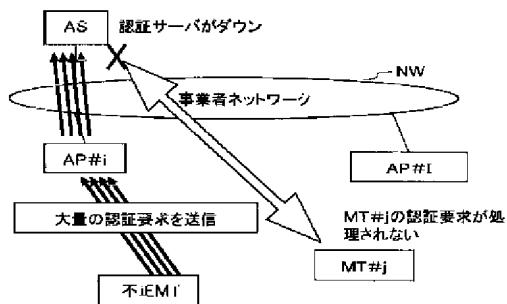
【図43】



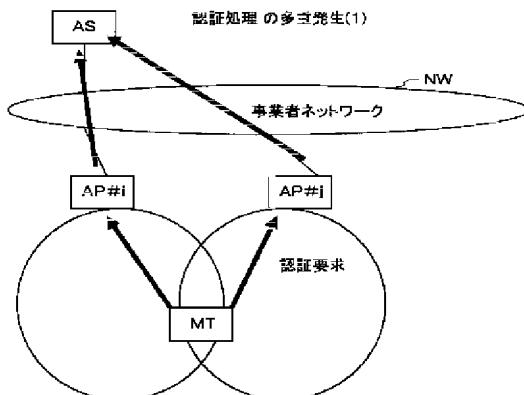
【図44】



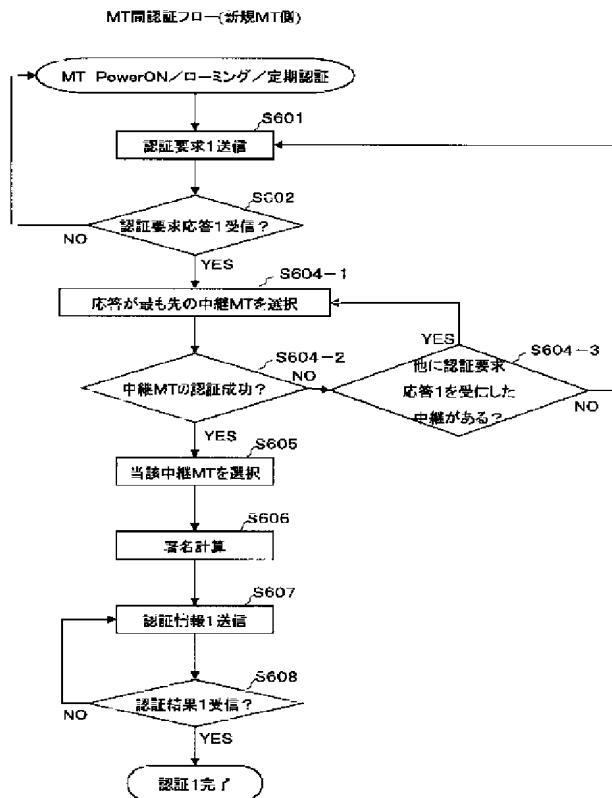
【図51】



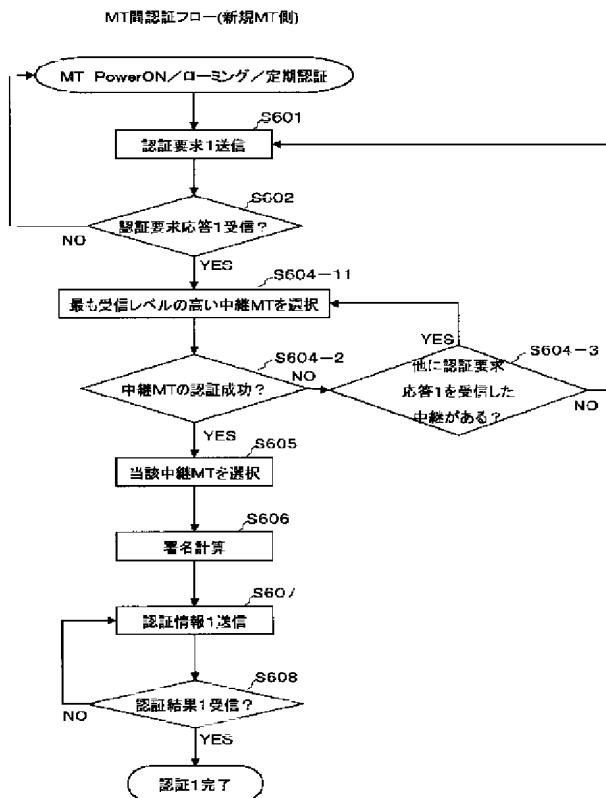
【図52】



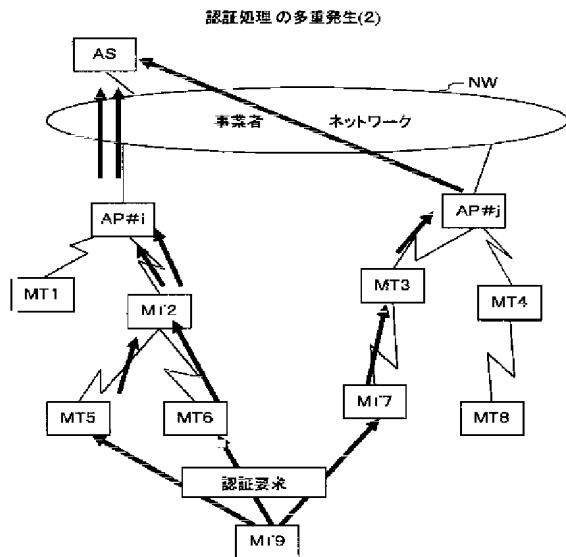
【図47】



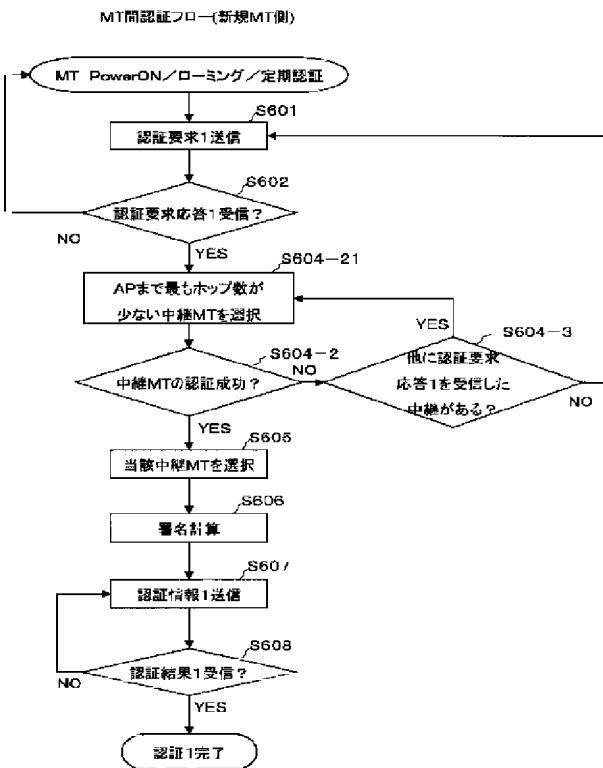
【図48】



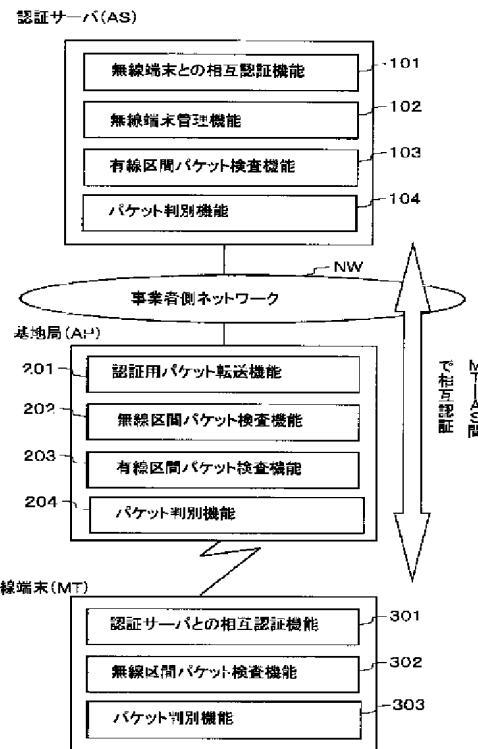
【図54】



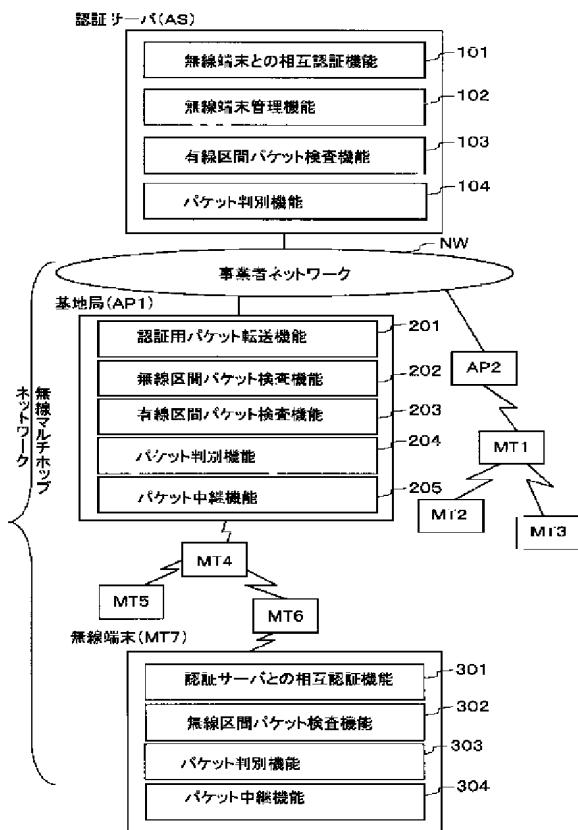
【図49】



【図50】



【図53】



フロントページの続き

(72)発明者 中山 正芳
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内

(72)発明者 須田 博人
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内

F ターム(参考) 5J104 AA07 KA02 MA01 PA07
 5K030 GA15 HA08 JL01 JT09 LB05
 5K067 AA32 BB02 BB21 CC08 DD17
 EE02 EE10 HH22 HH24 HH36